Installations- und Benutzerhandbuch - Deutsch

FUJITSU

FUJITSU Software ServerView Suite

ServerView-Agenten V7.10 für Windows

(Windows Server 2008/2012)

Ausgabe April 2015

Kritik...Anregungen...Korrekturen...

Die Redaktion ist interessiert an Ihren Kommentaren zu diesem Handbuch. Ihre Rückmeldungen helfen uns, die Dokumentation zu optimieren und auf Ihre Wünsche und Bedürfnisse abzustimmen.

Sie können uns Ihre Kommentare per E-Mail an manuals@ts.fujitsu.com senden.

Zertifizierte Dokumentation nach DIN EN ISO 9001:2008

Um eine gleichbleibend hohe Qualität und Anwenderfreundlichkeit zu gewährleisten, wurde diese Dokumentation nach den Vorgaben eines Qualitätsmanagementsystems erstellt, welches die Forderungen der DIN EN ISO 9001:2008 erfüllt.

cognitas. Gesellschaft für Technik-Dokumentation mbH

www.cognitas.de

Copyright und Handelsmarken

Copyright © 1998 - 2015 Fujitsu Technology Solutions.

Alle Rechte vorbehalten.

Liefermöglichkeiten und technische Änderungen vorbehalten.

Alle verwendeten Hard- und Softwarenamen sind Handelsnamen und/oder Warenzeichen der jeweiligen Hersteller.

Inhaltsverzeichnis

1 Einleitung **5**
1.1 Architektur 7
1.2 Zielgruppen und Zielsetzung des Handbuchs 11
1.3 Technische Voraussetzungen 11
1.3.1 Letzte Änderungen/Korrekturen 11
1.3.2 Verwalteter Server 11
1.4 Änderungen gegenüber der vorigen Ausgabe 12
1.5 ServerView Suite Link-Sammlung 12
1.6 Dokumentation zur ServerView Suite 14
1.7 Darstellungsmittel 14

2 Konfigurationen auf den verwalteten Servern **17**
2.1 BIOS und Firmware konfigurieren 19
2.1.1 Einstellungen im BIOS-Setup 20
2.2 Server konfigurieren 23
2.3 SNMP-Sicherheitskonzept 26
2.3.1 Einzelne SET-Operationen verbieten 27
2.3.2 SET-Operationen generell verbieten 27
2.3.3 SET-Operationen mit Benutzer-Authentifizierung 28
2.3.4 Betriebssystemspezifische Besonderheiten bei den ServerView-Agenten 30
2.4 SNMP-Dienste konfigurieren 30
2.4.1 Windows Server 2008/Windows Server 2012 32
2.4.2 Für Environment mit installiertem Server Core 35

3 Installation der ServerView-Agenten **37**
3.1 Agenten installieren und konfigurieren 38
3.2 Installierte Tools 56
3.3 RAID konfigurieren 60
3.4 APC- und Masterguard-USV konfigurieren 60
3.5 Installation über die Kommandoschnittstelle 63
3.6 Einstellungen nach der Installation 68
3.6.1 Administrativen Benutzer festlegen 68

3.6.2 Für Environment mit installiertem Server Core 70
3.7 Deinstallation 71
3.7.1 Windows Server 2008 72
3.7.2 Windows Server 2012 72
3.8 Neustart 72

1 Einleitung

Der ServerView Operations Manager (kurz: Operations Manager) ist ein kostenfreies Server-Management-Modul der Fujitsu ServerView Suite. Er steht Ihnen für die zentrale Server-Administration von Industrie Standard Servern zur Verfügung, die unter den Betriebssystemen Windows und Linux (SUSE und Red Hat) laufen oder als Host für VMs (Virtual Machine) dienen, die Hypervisor wie VMware ESXi, Citrix XenServer oder Hyper-V nutzen.

Die einheitliche Verwaltung aller Server erfolgt über eine oder auch mehrere zentrale Management-Stationen, auf die Sie von jeder Arbeitsstation im Netzwerk, auf der ein gängiger Web-Browser und das Java Runtime Environment laufen, zugreifen können.

Der Operations Manager kontrolliert die Einzelsysteme einschließlich kritischer Hardware-Komponenten, wie z. B. Prozessoren, Arbeitsspeicher, Festplatten, Lüfter und Stromversorgung. Er überwacht und steuert den Energieverbrauch, analysiert die Performanz- und Auslastungsdaten und aktualisiert die Serverkonfiguration.

Zum Sicherheitskonzept des Operations Manager gehört eine rollenbasierte Benutzerverwaltung, die auf drei grundlegenden Konzepten basiert:

- globale Benutzerverwaltung mithilfe eines LDAP-Verzeichnisdienstes (Lightweight Directory Access Protocol)
- rollenbasierte Zugangssteuerung (Role-Based Access Control, RBAC)
- Single Sign-on (SSO) auf Basis eines Centralized Authentication Service (CAS)

Mit RBAC können Sie Ihr Sicherheitskonzept an der Organisationsstruktur Ihres Unternehmens ausrichten, indem Sie jeder Rolle ein aufgabenorientiertes Berechtigungsprofil zuordnen.

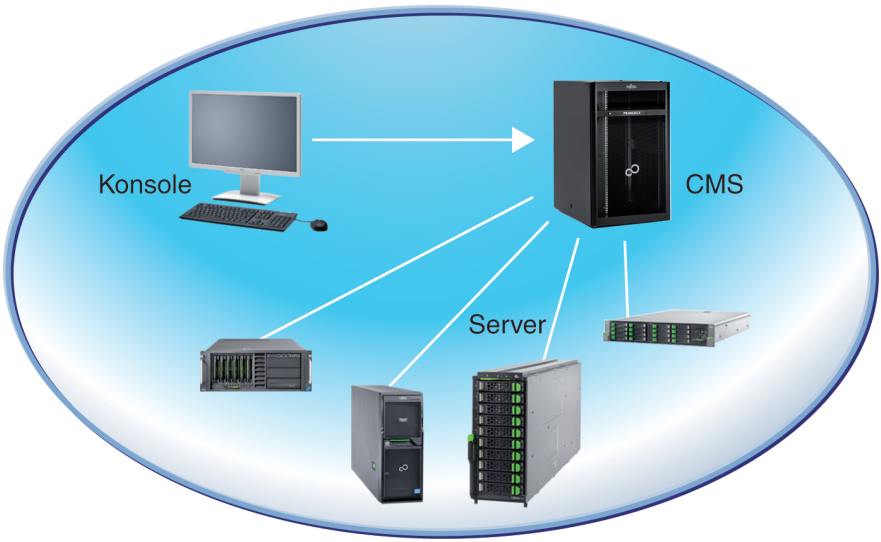
SSO bedeutet, dass Sie Ihre Authentizität nur einmal nachweisen müssen. Einmal erfolgreich authentifiziert, erhalten Sie Zugang zu allen ServerView-Komponenten, ohne sich bei einer dieser Komponenten neu anmelden zu müssen.

Das Server-Management mit dem Operations Manager bietet Betreibern eines umfangreichen Servernetzes entscheidende Vorteile:

- höhere Produktivität durch hohe Ausfallsicherheit der Server
- Senkung der Kosten durch automatisierte Überwachung der IT-Infrastruktur
- flexible Ausbaumöglichkeit der Server, da der Operations Manager problemlos an veränderte Bedingungen angepasst werden kann
- kürzere Ausfallzeiten durch vereinfachte Fehleranalyse
- Gewährleistung eines möglichst unterbrechungsfreien und energieeffizienten Serverbetriebs
- schnellere Reaktionszeiten im Falle eines Fehlers
- Senkung der Gesamtbetriebskosten (Total Cost of Ownership) durch effiziente Nutzung der Netzkomponenten und ihrer Ressourcen
- hohen Bedienkomfort durch Software-Ergonomie: übersichtliche Darstellung, intelligente Benutzerführung und unterstützendes Hilfesystem

1.1 Architektur

Die Architektur von ServerView Operations Manager basiert auf einer Management-Konsole, einer zentralen Management-Station (CMS) und den verwalteten Servern.



	Management-Konsole Eine Browser-basierte Management-Konsole ermöglicht die Verwaltung der Server und die Anzeige der ermittelten Daten. Die folgenden Browser können verwendet werden: • Microsoft Windows mit Internet Explorer oder Mozilla Firefox • SUSE/Red Hat Linux mit Standard-Web-Browser, der mit der Distribution freigegeben ist Das Java Runtime Environment muss auch installiert sein.

Zentrale Management-Station

Auf der zentralen Management-Station ist der ServerView Operations Manager installiert. Die optionalen Komponenten der ServerView Suite wie z. B. der Virtual IO-Manager werden ebenfalls auf der zentralen Management-Station installiert und in den Operations Manager integriert.

Die zentrale Management-Station und damit der ServerView Operations Manager und die zugehörigen Komponenten können auch auf einer virtuellen Maschine (VM) unter Windows oder Linux ausgeführt werden.

Das globale Benutzermanagement der ServerView Suite und des iRMC speichert die Benutzer zentral für alle zentralen Management-Stationen (CMS)/iRMC im Verzeichnis eines LDAP-Verzeichnisdienstes. Dadurch können Sie die Benutzer auf einem zentralen Server verwalten. Die Benutzer können daher von alle CMS und iRMC verwendet werden, die im Netzwerk mit diesem Server verbunden sind.

Die ServerView Suite unterstützt derzeit die folgenden Verzeichnisdienste:

- ApacheDS (unter JBoss 7).
- Microsoft Active Directory

Während der Installation von ServerView Operations Manager haben Sie die Möglichkeit, den internen Verzeichnisdienst (ApacheDS) von ServerView zu wählen. Weitere Informationen zur Nutzung der Verzeichnisdienste mit ServerView finden Sie im Handbuch "User Management in ServerView" (siehe).

Die Daten, die von ServerView erzeugt und genutzt werden, werden in einer SQL-Datenbank auf einem SQL-Server abgelegt. Die folgenden SQL-Server sind Teil der ServerView Operations Manager-Installation:

- SQL Server 2008 R2/2005 Express unter Windows Server
- PostgreSQL unter Linux

Es können aber andere Microsoft SQL Server Datenbanken unter Windows verwendet werden.

	Das Java Runtime Environment ist auf der zentralen Management-Station erforderlich. Wie Sie den ServerView Operations Manager installieren, wird in den folgenden Handbüchern beschrieben: • Installation ServerView Operations Manager Software unter Windows • Installation ServerView Operations Manager Software unter Linux
	Verwaltete Server Auf den verwalteten Servern müssen ServerView-Agenten, CIM Provider oder ServerView Agentless Service installiert sein, die die Informationen der zentralen Management-Station bereitstellen. Der ServerView RAID Manager und der ServerView Update Agent müssen auch auf den verwalteten Servern installiert werden. Die Installation der ServerView-Agenten auf virtuellen Maschinen (VMs) ist nicht freigegeben. • Die ServerView-Agenten sind verfügbar für Windows, Linux und Citrix XenServer. • ServerView CIM-Provider sind für Windows, Linux und VMware ESXi verfügbar. Der ServerView Operations Manager unterstützt aktuell nur ServerView CIM-Provider für VMware ESXi. Wie Sie diese installieren, ist in den folgenden Handbüchern beschrieben: • ServerView-Agenten für Windows • ServerView-Agenten für Linux • Installation ServerView ESXi CIM Provider • ServerView CIM-Provider für Windows, Linux und VMware ESXi

1.2 Zielgruppen und Zielsetzung des Handbuchs

Das vorliegende Handbuch wendet sich an Systemverwalter, Netzverwalter und Service-Fachleute, die über fundierte Hard- und Software-Kenntnisse verfügen. Das Handbuch beschreibt die Installation der ServerView-Agenten für Windows Server 2008 und Windows 2012.

1.3 Technische Voraussetzungen

1.3.1 Letzte Änderungen/Korrekturen

Eventuelle letzte Änderungen/Korrekturen der technischen Voraussetzungen finden Sie in der Readme-Datei auf der ServerView Suite DVD 2. Sie haben folgende Möglichkeiten:

- Wechseln Sie auf der DVD in das Verzeichnis **SVSSoftware** – **Software** – **ServerView** – **Windows** – **Agents**.
- Starten Sie die DVD und wählen Sie im Willkommen-Dialog **ServerView Software Products**; Info unter **ServerView** – **Agents and Providers**.

1.3.2 Verwalteter Server

ServerView-Agenten sind verfügbar für:

- Windows Server 2008
- Windows Server 2008 x64
- Windows Server 2008 R2
- Windows Server 2012 Datacenter
- Windows Server 2012 Standard
- Windows Server 2012 Foundation
- Windows Server 2012 R2 Datacenter
- Windows Server 2012 R2 Standard
- Windows Server 2012 R2 Foundation
- Windows Storage Server 2012 Standard

1.4 Änderungen gegenüber der vorigen Ausgabe

Diese Ausgabe des Handbuchs gilt für ServerView Agents V7.10 oder höher und ersetzt das Online-Handbuch "ServerView Agents V7.00 for Windows", Ausgabe Oktober 2014.

Das Handbuch enthält die folgenden Änderungen und Erweiterungen:

- Ab Version 7.10 unterstützt ServerView Operations Manager den Verzeichnisdienst ApacheDS anstelle von OpenDJ. Deshalb wurde der Architektur-Abschnitt aktualisiert, siehe "Architektur" auf Seite 7.
- Der Abschnitt "ServerView Suite Link-Sammlung" wurde aktualisiert, siehe "ServerView Suite Link-Sammlung" auf Seite 12.
- Ab ServerView Agents V7.01 ist die ServerView System Monitor Web-Oberfläche eine neue Funktion, die zusammen mit den Agenten installiert wird (siehe "Agenten installieren und konfigurieren" auf Seite 38, "Installation über die Kommandoschnittstelle" auf Seite 63 und "Installierte Tools" auf Seite 56).
- Ab Version 7.01 sind ServerView-Agenten in der Lage, einen Server über SNMPv3 zu überwachen. Deshalb wurde der Abschnitt "Konfigurationen auf den verwalteten Servern" auf Seite 17 aktualisiert. Siehe auch die neue Dokumentation "Usage of SNMPv3 with ServerView Agents 7.01".

1.5 ServerView Suite Link-Sammlung

Fujitsu Technology Solutions stellt Ihnen über die ServerView Suite Link-Sammlung zahlreiche Downloads und weiterführende Informationen zur ServerView Suite und zu PRIMERGY Servern zur Verfügung.

Zur ServerView Suite werden Ihnen Links zu folgenden Themen angeboten:

- Forum
- Service Desk
- Handbücher
- Produktinformationen
- Sicherheitsinformationen

- Software Downloads
- Schulungen

Die Downloads umfassen u. a.:

- Aktuelle Software-Stände zur ServerView Suite sowie ergänzende Readme-Dateien.
- Informationsdateien und Aktualisierungsdateien (Update Sets) für systemnahe Software-Komponenten (BIOS, Firmware, Treiber, ServerView-Agenten und ServerView-Update-Agenten) zur Aktualisierung der PRIMERGY Server anhand des ServerView Update Managers oder für den lokalen Update einzelner Server anhand des ServerView Update Managers Express.
- die aktuellen Versionen aller Dokumentationen zur ServerView Suite

Die Downloads können kostenlos vom Fujitsu Technology Solutions Web-Server heruntergeladen werden.

Zu PRIMERGY Servern werden Ihnen Links zu folgenden Themen angeboten:

- Service Desk
- Handbücher
- Produktinformationen
- Ersatzteilkatalog

Zugriff auf die ServerView Suite Link-Sammlung

Die Link-Sammlung der ServerView Suite erreichen Sie über verschiedene Wege:

1. Über den ServerView Operations Manager.
   - Wählen Sie auf der Startseite bzw. in der Menüzeile **Help** – **Links** aus.

Anschließend wird die Startseite der ServerView Suite Link-Sammlung angezeigt.

2. Über die Startseite der Online-Dokumentation zur ServerView Suite auf dem Manual-Server von Fujitsu Technology Solutions.

Sie gelangen auf die Startseite der Online-Dokumentation mit folgendem Link:

http://manuals.ts.fujitsu.com

- Wählen Sie links in der Auswahlliste **x86 Servers**.

- Klicken Sie rechts unter **Selected documents** auf **PRIMERGY ServerView Links**.

Anschließend wird die Startseite der ServerView Suite Link-Sammlung angezeigt.

3. Über die ServerView Suite DVD 2.
   - Wählen Sie im Startfenster der ServerView Suite DVD 2 die Option **ServerView Software Produktauswahl**.
   - Wählen Sie in der Menüleiste **Links**.

Anschließend wird die Startseite der ServerView Suite Link-Sammlung angezeigt.

1.6 Dokumentation zur ServerView Suite

1.7 Darstellungsmittel

Es werden folgende Darstellungsmittel verwendet:

Darstellungsmittel	Bedeutung
	Weist auf Gefahren hin, die zu Gesundheitsgefährdung, Datenverlust und Geräteschäden führen können.
	Verweist auf weiterführende Informationen und Tipps.
Fette Schrift	Kennzeichnet Bildschirmzitate der Namen der Oberflächenelemente.
`dicktengleich`	Kennzeichnet Ausgaben des Systems und Systemelemente wie Dateinamen oder Pfade.
`dicktengleich halbfett`	Kennzeichnet Anweisungen, die Sie über die Tastatur eingeben.
blauer, unterstrichener Text	Kennzeichnet einen Link zu einem verwandten Thema.
lila, unterstrichener Text	Kennzeichnet einen besuchten Link.

Darstellungsmittel	Bedeutung
<abc>	Kennzeichnet Variablen, die Sie durch reale Werte ersetzen müssen.
[abc]	Kennzeichnet Optionen, die Sie angeben können (Syntax).
[Taste]	Kennzeichnet eine Taste entsprechend ihrer Abbildung auf der Tastatur. Wenn Sie explizit Großbuchstaben eingeben sollen, dann wird die Shift-Taste angegeben, z. B. [SHIFT] + [A] für A. Wenn Sie zwei Tasten gleichzeitig drücken sollen, kennzeichnet dies ein Pluszeichen zwischen den Tastensymbolen.

Bildschirmabzüge

Die Bildschirmabzüge sind teilweise systemabhängig und müssen deshalb nicht in allen Details mit der Ausgabe auf Ihrem System übereinstimmen. Auch bei den Menüs und ihren Befehlen kann es systembedingte Unterschiede geben.

2 Konfigurationen auf den verwalteten Servern

Bevor Sie den Operations Manager in Betrieb nehmen können, müssen auf dem verwalteten Server folgende Vorbereitungen getroffen werden:

- Nur für PRIMERGY: Im BIOS jedes verwalteten Servers müssen bestimmte Einstellungen vorgenommen werden, siehe "BIOS und Firmware konfigurieren" auf Seite 19.

  Auf jedem Server müssen Sie Konfigurationseinstellungen vornehmen, siehe "Server konfigurieren" auf Seite 23.
- ServerView bietet ein differenziertes Sicherheitskonzept. Bevor Sie die Agenten installieren, sollten Sie sich über das Sicherheitskonzept informieren und das Ihrem Sicherheitsbedürfnis entsprechende Konzept auswählen. Gegebenenfalls müssen Sie vor der Installation der Agenten entsprechende Vorbereitungen treffen. Dies wird beschrieben unter "SNMP-Sicherheitskonzept" auf Seite 26.
- Sie müssen die SNMP-Dienste des jeweiligen Betriebssystems auf jedem verwalteten Server und der Management-Station installieren und konfigurieren. Andernfalls kann die Management-Station die Server nicht überwachen. Die SNMP-Dienste müssen je nach Betriebssystem vor bzw. nach der Agenteninstallation aktiviert werden. Dies wird beschrieben unter "SNMP-Dienste konfigurieren" auf Seite 30.
- Ab Version 7.01 sind ServerView-Agenten in der Lage, einen Server über SNMPv3 zu überwachen.

  Um SNMPv3 zum Verwalten eines Windows-basierten Servers nutzen zu können, muss der SNMP-Dienst von Microsoft Windows ersetzt werden. Als Ersatz für den SNMP-Dienst von Microsoft Windows empfiehlt sich der Net-SNMP-Master Agent (siehe Beschreibung unter "Usage of SNMPv3 with ServerView Agents 7.01").
- ServerView-Agenten müssen auf jedem zu verwaltenden Server installiert sein, siehe "Installation der ServerView-Agenten" auf Seite 37.

Die Installation der ServerView-Agenten auf virtuellen Maschinen (VMs) ist nicht freigegeben.

Für die RXI-Server gibt es spezielle ServerView-Agenten, die mit dem Server auf einer gesonderten IA 64 ServerSupport CD ausgeliefert werden.

- Voraussetzung für den ServerView Update Manager ist, dass auf den verwalteten Servern der ServerView-Update-Agent installiert ist. Die Installation wird beschrieben im Benutzerhandbuch "ServerView Update Management".
- Wenn der ServerView Operations Manager so konfiguriert wurde, dass der Zugriff auf die zentrale Management-Station nicht über den Namen sondern über die IP-Adresse erfolgt, muss gewährleistet sein, dass vom verwalteten Server über diese Adresse auf die zentrale Management-Station zugegriffen werden kann. Das sollte möglichst durch eine entsprechenden Eintrag in das DNS geschehen. Wenn kein DNS verfügbar ist, müssen Sie den entsprechenden Eintrag in der Datei **hosts** auf dem verwalteten Server erstellen. In Windows finden Sie diese Datei im Verzeichnis **%WINDIR%\system32\drivers\etc**.

Zusätzliche Installation auf den verwalteten Server

- ServerView RAID Manager

  Der ServerView RAID Manager bietet eine einheitliche Administration und Verwaltung von Festplatten für PRIMERGY Server. Ohne Installation des ServerView RAID Managers sind keine Informationen über RAID-Laufwerke und deren Zustand verfügbar.

  Die Installation ist im Benutzerhandbuch "RAID Management" beschrieben.

- ServerView Online Diagnostics

  Bei der Installation der ServerView-Agenten für Windows wird Online Diagnostics mit installiert. Mit Online Diagnostics können Sie vom Remote-Arbeitsplatz aus eine Reihe von Hardware-Tests auf einem verwalteten PRIMERGY Server durchführen.

- Bei der Installation der ServerView-Agenten (für Windows) im Expertenmodus können Sie auswählen, ob zusätzliche Komponenten mit

installiert werden sollen, u.a. Asset CLI, Configuration Tools, Prime Collect, ServerView System Monitor und ServerView CIM Provider.

- Mithilfe von ServerView System Monitor können Sie Serverinformationen lokal auf dem Server überwachen und überprüfen. ServerView System Monitor wird beschrieben im Benutzerhandbuch "ServerView System Monitor".
- Die ServerView CIM Provider stehen für das Management von PRIMERGY Servern über die CIM Infrastruktur zur Verfügung.

  Falls das Betriebssystem CIM Provider nicht unterstützt, wird unter **Custom Setup** die Funktionalität ServerView CIM Provider nicht angeboten.

  Nähere Informationen finden Sie im Handbuch "ServerView CIM Providers for the management of PRIMERGY servers", das die von den ServerView CIM Providern unterstützen Profile detailliert beschreibt.

2.1 BIOS und Firmware konfigurieren

Die folgende Beschreibung ist nur gültig für PRIMERGY.

Abhängig von der Systembaugruppe arbeiten die verschiedenen PRIMERGY-Typen mit unterschiedlichen BIOS-Versionen. Deshalb wird auf die detaillierte Beschreibung aller möglichen Einstellungen sowie der Bedienung des BIOS an dieser Stelle verzichtet.

Eine ausführliche Beschreibung der jeweiligen BIOS-Version finden Sie im Referenzhandbuch "BIOS Setup Utility" oder im technischen Referenzhandbuch der Systembaugruppe.

Bei der Inbetriebnahme eines Servers müssen Sie den Menüpunkt **O/S Boot Timeout** im BIOS-Setup des Systems auf **Disabled** stellen. Sonst wird das System während der Installation neu gestartet.

Erst beim Neustart des Systems, wenn alle Installationen abgeschlossen sind (einschließlich der ServerView-Agenten), können Sie den Menüpunkt **O/S Boot Timeout** auf **Enabled** stellen.

2.1.1 Einstellungen im BIOS-Setup

Die Server-Management-Firmware überwacht den Server, bis das Betriebssystem gestartet ist. Danach übernehmen die Agenten und der Operations Manager die Überwachungsfunktion.

Sie müssen die BIOS-Einstellungen auf jedem Server vornehmen.

Rufen Sie das BIOS-Setup auf, indem Sie den Rechner neu starten und in der Boot-Phase an entsprechender Stelle die Taste **F2DEL** oder drücken.

Wählen Sie im BIOS-Setup das Menü **Server** aus. Hier nehmen Sie die Einstellungen zum Server-Management vor.

Wird im BIOS-Setup das Menü **Server** nicht angeboten, so brauchen Sie die Server-Management-Funktionen nicht zu aktivieren. Allerdings können dann auch einzelne Server-Management-Funktionen nicht explizit gesteuert werden.

Wird im Menü **Server** der Menüpunkt **Server Management** angeboten, so wählen Sie für diesen Menüpunkt die Einstellung **Enabled** aus. Dadurch wird die Server-Management-Funktionalität aktiviert. Alle weiteren Einstellungen werden nur dann wirksam, wenn Sie hier die Einstellung **Enabled** auswählen.

Steht der Menüpunkt **Server Management** nicht zur Verfügung, können die einzelnen Funktionen unabhängig von einer generellen Freigabe gesteuert werden.

Im Menü **Server** stehen die im Folgenden aufgeführten Felder zur Verfügung.

Beachten Sie, dass, abhängig von der Hardware, nicht alle Felder zur Verfügung stehen müssen.

O/S Boot Timeout

Hier legen Sie fest, ob ein Systemneustart erfolgen soll, wenn das Betriebssystem nach dem Systemstart nicht in einer vorgegebenen Zeitspanne Verbindung mit der Server-Management-Firmware aufnimmt.

Das Zeitintervall kann auch über den Operations Manager festgelegt werden (siehe auch im Benutzerhandbuch "ServerView Operations Manager" den Abschnitt "ASR&R").

Inbetriebnahme des Servers

Bei der Inbetriebnahme des Servers müssen Sie den Menüpunkt **O/S Boot Timeout** auf **Disabled** stellen. Sonst wird das System während der Installation neu gestartet.

Aktion nach Zeitablauf

Legt fest, welche Aktion nach Ablauf des Boot-Watchdogs ausgeführt wird.

Timeout Value

Legt die Zeit fest, nach der ein Neustart des Systems erfolgt, falls dies über **O/S Boot Timeout** eingeschaltet ist.

ASR&R Boot Delay

Legt die Zeitspanne fest, die der Server nach einer Fehlerabschaltung (z.B. wegen Übertemperatur) wartet, ehe er einen Neustart durchführt.

Boot Retry Counter

Legt fest, wie oft der Server versucht das Betriebssystem neu zu starten, bevor er abgeschaltet bleibt bzw. bevor ServerView Remote Management gestartet wird.

Diagnostic System

Legt fest, ob ServerView Remote Management gestartet wird, wenn die unter **Boot Retry Counter** eingestellte Anzahl an Systemneustarts erreicht ist.

Hardware Watchdog

Legt fest, ob der Server einen Neustart durchführt, wenn das Server-Management-BIOS einen Hardware-Zähler nicht in bestimmten Zeitintervallen zurücksetzen kann.

Next Boot uses

Legt fest, ob beim nächsten Boot-Vorgang ServerView Remote Management gestartet wird.

Temperature Monitoring

Legt fest, ob das System abgeschaltet wird, wenn die Temperatur den kritischen Wert überschreitet.

Memory Scrubbing

Legt fest, ob der Speicher überprüft und Ein-Bit-Fehler beseitigt werden.

BIOS Runtime Logging

Legt fest, ob Prozessor-, Speicher- oder PCI-Fehler in der Error-Log-Datei gespeichert werden.

CPU Status

Legt fest, ob der Prozessor verwendet werden kann.

Memory Status

Hier können bestimmte Speichermodule als fehlerhaft gekennzeichnet werden. Diese werden dann beim nächsten Systemstart nicht mehr verwendet.

Console Redirection

Legt die Einstellungen zum Betrieb eines Terminals am System fest.

RomPilot

Legt die Einstellungen zu RomPilot fest. RomPilot ist ein Bestandteil von ServerView Remote Management und des Operations Managers. Mit RomPilot ist der Remote-Zugriff von einer Remote-Konsole über LAN auf die Systemstartphase (POST) und MS-DOS möglich.

Storage Extension

Legt die Einstellungen für die Gruppenkonfiguration und den Kommunikationsbus (CAN-Bus) fest. (Hinweis: **Storage Extension** gibt es nicht auf allen Servern!)

2.2 Server konfigurieren

Zur Konfiguration von Servern stehen Ihnen verschiedene Funktionen zur Verfügung. Während einige dieser Funktionen für alle PRIMERGY Server unterstützt werden, werden andere Funktionen je nach Hard- und Software-Ausstattung der PRIMERGY Server nur für bestimmte Server angeboten.

Die Konfiguration der Server können Sie vornehmen:

- Lokal am verwalteten Server über den Server Configuration Manager.

  Mit dem Server Configuration Manager können Sie Einstellungen zum allgemeinen Systemverhalten des Zielsystems vornehmen und - sofern vorhanden - die Remote Management-Komponente (iRMC oder iRMC S2/S3) des Zielsystems konfigurieren.

  Wenn der ServerView Installation Manager über die ServerView Suite DVD 1 gestartet wird, können Sie den Server Configuration Manager über die Schaltfläche **Server Configuration Manager** starten.

  Abhängig vom PRIMERGY Server-Typ des Zielsystems werden nicht alle Schritte durchlaufen. Die Reihenfolge der einzelnen Schritte sowie die Konfigurationsmöglichkeiten in den einzelnen Schritten können ebenfalls von System zu System variieren.

  Nähere Informationen zu den individuellen Schritten im Konfigurationsdialog des Server Configuration Managers finden Sie in der Online-Hilfe zum Server Configuration Manager.

  Um die Online-Hilfe zu einem Schritt im Dialog aufzurufen, gehen Sie vor wie folgt:

  1. Klicken Sie in den Anzeigebereich, in dem der Dialog angezeigt wird.
  2. Drücken Sie die Taste F1.

- Auf Windows Server 2008: Lokal am verwalteten Server über das **Start** Menü.

  Wählen Sie auf dem verwalteten Server **Start** – **All Programs** – **Fujitsu** – **ServerView Suite** – **Agents** – **System Configuration**.

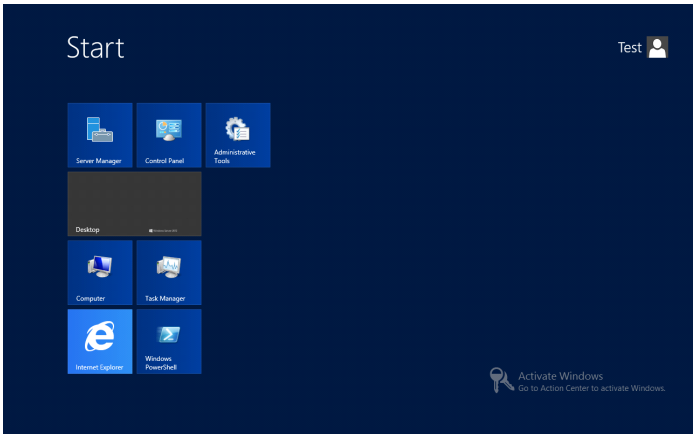
  Die Konfiguration können Sie nur für Server vornehmen, auf denen die ServerView-Agenten installiert sind.

  Einzelheiten zu den jeweiligen Serverkonfigurationsschritten finden Sie in der Online-Hilfe.

  Um die Online-Hilfe zu einem Schritt im Dialog aufzurufen, gehen Sie vor wie folgt:

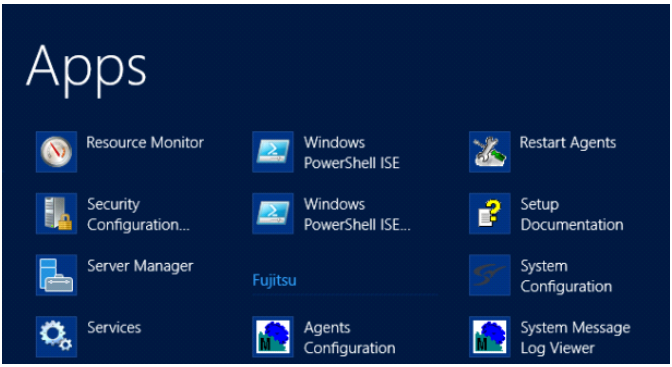
  1. Klicken Sie in den Anzeigebereich, in dem der Dialog angezeigt wird.
  2. Drücken Sie die Taste F1.

- Auf Windows Server 2012: Lokal am verwalteten Server über die **Start** Seite:



  1. Es gibt verschiedene Möglichkeiten die Server zu konfigurieren. Eine Möglichkeit ist, auf die **Apps** Seite zu wechseln. Um diese Seite zu öffnen, klicken Sie auf die rechte obere oder untere Ecke auf der **Start** Seite. In dem angezeigten Fenster wählen Sie **Search**.

2. Wählen Sie **System Configuration** auf der **Apps** Seite.



- Über den ServerView Configuration Manager, der in die grafische Oberfläche des Operations Managers integriert ist. Damit können Sie den Server via Web-Interface auch vom Remote-Arbeitsplatz aus konfigurieren können.

  ServerView Configuration Manager kann über die Startseite von Operations Manager oder durch die Auswahl von **Administration** – **Server Configuration** in der Menüleiste gestartet werden.

  Weitere Informationen finden Sie im Benutzerhandbuch "ServerView Operations Manager".

  Die Konfiguration können Sie nur für Server vornehmen, auf denen die ServerView-Agenten installiert sind.

Einige der konfigurierten Einstellungen werden je nach System ins BIOS übernommen.

Sie können u.a. folgende Einstellungen vornehmen:

- Lesen der wichtigsten Daten des Servers, der Systembaugruppe und des integrierten Management Controllers
- Lesen und Setzen der Boot- und Software-Watchdog-Einstellungen
- Lesen und Bearbeiten des Fehlerzählers für die Speichermodule

Nur für PRIMERGY

- Lesen und Löschen des Error- und Event-Logs des Servers
- Überwachung und Kalibrierung der Systemlüfter
- Lesen und Setzen der Gehäusekennzeichnung (bei Auslieferung voreingestellt)
- Lesen und Zurücksetzen der Zähler über die Systemlaufzeiten
- Konfigurieren der Einstellungen für HTTP und Telnet und der Einstellung des Remote Management Controllers für HTTP
- Konfigurieren der IP- und DNS-Einstellungen der RSB Web-Oberfläche
- Konfigurieren der SNMP-Communities und der Trap-Ziele für die SNMP-Schnittstelle des Remote Management Controllers
- Verwalten der Benutzerkennungen des Remote Management Controllers
- Konfigurieren der seriellen Schnittstelle des RSBs bzw. des Remote Management Controllers
- Konfigurieren der Operations Manager USV-Management-Integration
- Konfigurieren der Anzeigen auf dem ServerView Local Service Display

2.3 SNMP-Sicherheitskonzept

Die ServerView-Agenten bieten in Verbindung mit dem ServerView-Manager ein erweitertes Sicherheitskonzept, um unerlaubte SNMP-SET-Operationen auf einem Server zu verhindern.

Sie können SNMP-SET-Operationen auf dem Server einschränken. Hierbei besteht die Möglichkeit:

- einzelne SET-Operationen zu verbieten,
- SET-Operationen generell zu verbieten,
- SET-Operationen durch eine Benutzer-Authentifizierung zu schützen.

Ist die Benutzer-Authentifizierung aktiviert, so wird vor jeder Ausführung einer SET-Operation eine Benutzer-Authentifizierung durchgeführt. Verläuft diese erfolgreich, so wird zusätzlich die Zugehörigkeit zu einer vom Administrator vergebenen Benutzergruppe überprüft.

Die Benutzer-Authentifizierung funktioniert nur mit dem ServerView-Manager. Es ist für andere SNMP-Tools wirkungslos.

Weiterhin können Sie die Sicherheit vor unerlaubtem Zugriff erhöhen, indem Sie die Standardkonfiguration des SNMP-Dienstes ändern. Weitere Informationen finden Sie unter "SNMP-Dienste konfigurieren" auf Seite 30.

2.3.1 Einzelne SET-Operationen verbieten

Einige SET-Operationen bewirken einen Shutdown oder Neustart des Systems. Sie können diese speziellen SET-Operationen zulassen oder verbieten.

Welche Angaben Sie bei der Agenteninstallation machen müssen, um SET-Operationen zu verbieten, ist abhängig von dem Betriebssystem, unter dem der ServerView-Agent installiert wird, sowie von der Version des ServerView-Agenten. Eine genaue Beschreibung finden Sie auf "Installation der ServerView-Agenten" auf Seite 37.

2.3.2 SET-Operationen generell verbieten

Sie können SET-Operationen generell für die ServerView-Agenten verbieten. Geben Sie diese Spezifikationen bei der Agenten-Installation ein.

Welche Angaben Sie bei der Agenteninstallation machen müssen, um SET-Operationen zu verbieten, ist abhängig von dem Betriebssystem, unter dem der ServerView-Agent installiert wird, sowie von der Version des ServerView-Agenten. Eine genaue Beschreibung finden Sie auf "Installation der ServerView-Agenten" auf Seite 37.

Diese Option gilt nur für ServerView-Agenten. SET-Operationen für andere SNMP-Agenten werden davon nicht beeinflusst.

2.3.3 SET-Operationen mit Benutzer-Authentifizierung

Sie haben die Möglichkeit, SET-Operationen abzusichern, indem Sie die Ausführung einer SET-Operation durch eine Benutzer-Authentifizierung absichern. Hierbei können Sie einstellen, ob die Benutzerabfrage nur zu Beginn einer Sitzung für einen Server angegeben werden muss oder bei jeder SET-Operation erneut abgefragt wird.

Für die Benutzer-Authentifizierung müssen Sie Maßnahmen auf dem verwalteten Server sowie an der Management-Station vornehmen.

Instanz	Maßnahme
Verwalteter Server	• Benutzer und Benutzergruppe festlegen • Benutzer der gewünschten Benutzergruppe zuordnen • bei der Agenteninstallation die gewünschte Benutzergruppe angeben
Management-Station	im Operations Manager auf der Registerkarte **Login** den Benutzer angeben

Benutzer und Benutzergruppe definieren und Benutzer zuordnen
Den Benutzer sowie die Benutzergruppe müssen Sie mit Betriebssystemmitteln auf dem jeweiligen Server festlegen. Sie können für den Benutzernamen sowie für die Benutzergruppe einen beliebigen Namen (z. B. auch **Administrator**) auswählen.

Vorbereitend müssen Sie sich überlegen, ob Sie für mehrere Server die gleiche Benutzerkennung und -gruppe einrichten wollen oder nicht.

Benutzergruppe bei der Agenteninstallation angeben
Bei der Agenteninstallation auf dem Server müssen Sie die Benutzergruppe angeben, zu der der Benutzer gehören muss, für den SET-Operationen zugelassen sind. Die Installation und Konfiguration der ServerView-Agenten sind je nach Betriebssystem und Version unterschiedlich. Weitere Informationen zur Installation und Konfiguration in diesen Fällen finden Sie bei den Agenten-Beschreibungen beginnend ab Seite 45.

Benutzer an der Management-Station angeben

An der Management-Station müssen Sie im Operations Manager den Benutzer für einen Server angeben, der SET-Operationen auf dem jeweiligen Server durchführen darf. Bei einer SET-Operation wird dann der Benutzer abgefragt. Sie legen den Benutzer über die Registerkarte **Login** im Eigenschaftsfenster **Server Properties** fest. In diesem Beispiel wäre das der Benutzer **SVUSER**.

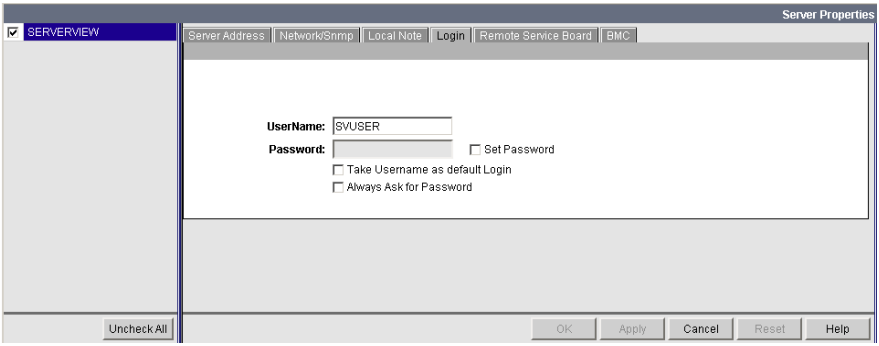


Bild 1: Benutzer-Authentifizierung

Aus Sicherheitsgründen ist es sinnvoll, falls ein Passwort für den Benutzer vergeben wurde, das Passwort hier ebenfalls anzugeben (**Set Password**). Weiterhin legen Sie mit **Always Ask for Password** fest, ob der Benutzername und das Passwort bei jeder Änderung der Einstellungen oder nur bei der ersten Änderung nach dem Programmstart des Operations Managers abgefragt werden sollen. Sie erreichen eine erhöhte Sicherheit, indem Sie die Funktion **Always Ask for Password** einschalten, weil in dem Fall das Passwort nicht abgespeichert wird.

Auf der linken Spalte im Eigenschaftsfenster können Sie diejenigen Server auswählen, für die die Einstellungen gelten sollen. Sie können auch mehrere gleichzeitig auswählen. Das heißt, Sie können die Einstellungen sowohl für jeden einzelnen Server individuell als auch für mehrere Server identisch vornehmen.

Das Öffnen des Eigenschaftsfenster wird beschrieben im Benutzerhandbuch "ServerView Operations Manager".

2.3.4 Betriebssystemspezifische Besonderheiten bei den ServerView-Agenten

Die folgenden Abschnitte beschreiben die betriebssystemspezifische und versionsabhängige Vorgehensweise bei der Umsetzung des Sicherheitskonzepts von ServerView.

SNMP-Sicherheitskonzept
Die Konfiguration der Sicherheitseinstellungen nehmen Sie bei Windows während der Installation der ServerView-Agenten vor:

- Sie können SET-Operationen für die ServerView-Agenten erlauben bzw. verbieten. Wenn Sie SET-Operationen verbieten, werden alle SNMP-SETs unabhängig von dem zur Ausführung verwendeten SET-Tool abgelehnt. (Anzeige auf der Management-Station in Operations Manager auf den Registerkarten **Restart Settings** und **Power ON/OFF** bei den Einstellungen unter **Set Enabled on server**)

  Diese Option gilt nur für ServerView-Agenten. SET-Operationen für andere SNMP-Agenten werden davon nicht beeinflusst.

- Sie können die Benutzer-Authentifizierung für SET-Operationen ein- bzw. ausschalten. Sie können die Benutzergruppe angeben, zu der die Benutzer gehören müssen, die SET-Operationen auf dem Server ausführen dürfen.
- Einige SET-Operationen (z. B. **Restart**/**Shutdown**/**Abort Shutdown** im Fenster **Recovery**) verursachen ein Herunterfahren oder einen Neustart des Systems. Sie können diese speziellen SET-Operationen zulassen oder verbieten.

Weitere Informationen zur Installation der Agenten finden Sie unter "Installation der ServerView-Agenten" auf Seite 37.

2.4 SNMP-Dienste konfigurieren

Sie müssen die SNMP-Dienste auf jedem verwalteten Server und jeder Management-Station installieren und konfigurieren.

Bei der Installation und Konfiguration der SNMP-Dienste werden Ihnen Standardwerte angeboten. Sie können die Standardwerte des SNMP-Dienstes

modifizieren. Falls Sie die Werte ändern, müssen Sie daran denken, auf der Management-Station die Werte entsprechend zu ändern.

Folgende Werte werden konfiguriert:

- Communityname für empfangene SNMP-Anfragen

  Der Communityname ist Bestandteil eines jeden SNMP-Requests, der vom Manager an den Agenten geschickt wird.

  Nach der Installation des SNMP-Dienstes gibt es keine Community. Sie sollten den Communitynamen **public** vergeben. Dieser Standardwert wird von den meisten SNMP-Diensten genutzt. Es ist aus Sicherheitsgründen sinnvoll, den Wert zu ändern. Im Prinzip können Sie für jeden Server bzw. für Servergruppen eine individuelle Community definieren. Denken Sie daran, Änderungen, die Sie hier vornehmen, auch auf der Management-Station durchzuführen.

  - Bei der Eingabe des Community-Namen wird zwischen Groß- und Kleinschreibung unterschieden.
  - Die Community-Namen können konfiguriert werden. Das Vorgehen dazu ist im White Paper "Secure PRIMERGY Server Management" beschrieben.

- Sicherheit

  Als Sicherheitsmerkmal für den SNMP-Zugriff können Rechte zugeordnet werden (z.B. **NUR LESEN**, **LESEN SCHREIBEN**). Wenn Sie die gesamte Operations Manager Funktionalität nutzen wollen, müssen Sie der Community das Recht **LESEN SCHREIBEN** vergeben. Sie können die Funktionalität einschränken, indem Sie nur lesenden Zugriff zulassen (**NUR LESEN**).

  Der ServerView-Manager unterstützt pro Server nur eine Community für SNMP-Requests. Deshalb können Sie keine verschiedenen Communities mit unterschiedlichen Rechten für einen Server konfigurieren.

- SNMP-Pakete von jedem Host annehmen

  Es wird empfohlen, nur die IP-Adresse des Servers einzugeben, der als zentrale Management-Station fungieren soll. Damit wird verhindert, dass der Agent Anfragen von nicht berechtigten Servern akzeptiert.

Wenn Sie den Zugriff auf dedizierte zentrale Management-Stationen beschränken, sollten Sie der Liste zugelassener Server auch den verwalteten Knoten selbst hinzufügen (über dessen eigene IP-Adresse oder "localhost"). Dies ist erforderlich, weil die Agenten auf der zentralen Management-Station Daten von anderen SNMP-Agenten auf diesem Server anfordern (erforderlich für den Berichts- und den Inventur-Agenten).

- Trapziele

  IP-Adresse der Management-Station, an den die ServerView-Agenten Traps senden.

- Communityname

  Hier geben Sie den Community-Namen an, der als Teil eines SNMP-Traps an die Management-Station geschickt wird. Der SNMP-Dienst auf der Management-Station muss so konfiguriert werden, dass er Traps mit diesem Community-Namen akzeptiert.

Achten Sie bitte darauf, wann die Installation und Konfiguration der SNMP-Dienste erfolgen muss. Dies hängt von dem Betriebssystem ab, welches Sie benutzen. Je nach vorliegendem Betriebssystem erfolgt die Installation und Konfiguration der SNMP-Dienste vor oder nach der Installation der Agenten.

2.4.1 Windows Server 2008/Windows Server 2012

Wenn Sie Windows Server 2008 oder Windows Server 2012 auf dem Server installiert haben und bevor Sie die ServerView-Agenten installieren, müssen Sie folgende Schritte vornehmen, sofern Sie dies nicht bereits während der Systeminstallation durchgeführt haben:

1. **SNMP Installation**

   Für die Installation unter Windows Server 2008:

   1. Wählen Sie **Start** – **Control Panel** – **Administrative Tools** – **Server Manager**.
   2. Klicken Sie im Fenster **Server Manager** auf **Features**. Wird **SNMP Services** nicht aufgelistet, dann klicken Sie auf **Add Features**.
   3. Aktivieren Sie die Option **SNMP Services** und klicken Sie auf **Next**.

4. Im Fenster **Confirm Installation Selections** klicken Sie auf **Install**.
5. Nach erfolgreicher Installation klicken Sie auf **Close**.

Für die Installation unter Windows Server 2012:

1. Wechseln Sie zur **Start**-Seite von Windows.
2. Starten Sie das Dashboard von **Server Manager**.
3. Klicken Sie auf **Add roles and features**.
4. Wählen Sie die Installationsoption **Role-based** oder **feature-base** und klicken Sie auf **Next**.
5. Wählen Sie den zu verwaltenden Server aus und klicken Sie auf **Next**.
6. Ignorieren Sie die Seite **Server Roles** und klicken Sie einfach auf **Next**.
7. Suchen Sie auf der Seite **Features** nach **SNMP Service**.
8. Falls das Feature **SNMP Service** nicht installiert ist, wählen Sie es aus und klicken Sie auf **Next**.
9. Klicken Sie auf **Install**, um die Installation des SNMP-Dienstes abzuschließen.
10. Sie können das Installationsfenster jederzeit schließen, ohne die laufenden Aufgaben zu unterbrechen.

2. SNMP Konfiguration
   1. Auf Windows Server 2008: Klicken Sie auf **Start** – **Control Panel** – **Administrative Tools** – **Server Manager**, um Server-Manager aufzurufen (falls nicht bereits geöffnet). Doppelklicken Sie **Configuration** und klicken Sie dann **Services**.

      Auf Windows Server 2012: Wählen Sie auf der Seite **Server Manager** die Option **Tools** – **Services**.
   2. Markieren Sie den Dienst **SNMP Service** und wählen Sie aus dem Kontextmenü den Eintrag **Properties**.
   3. Wählen Sie im Fenster **SNMP Service Properties** die Registerkarte **Traps**.
   4. Tragen Sie auf der Registerkarte **Traps** unter **Community name** einen Namen ein, oder bestätigen Sie den Standardeintrag **public**.

      In einigen Fällen existiert die Community **public** nicht.

Mit **Communityname** wird die Zugriffsberechtigung der Management-Station gesteuert. Nur eine Management-Station, die der hier eingetragenen Community angehört, darf den Server abfragen. Wenn Sie nicht **public** wählen, müssen Sie die Community in der Management-Station für den betreffenden Server ebenfalls ändern.

5. Tragen Sie unter **Trap destinations** mit **Add...** die IP-Adresse oder den Domainnamen der Management-Station für die angegebene Community ein.

   Traps werden nur an die hier eingetragene Management-Station gesendet.

6. Klicken Sie auf **OK**.

3. SNMP Sicherheit
   1. Wählen Sie im Fenster **SNMP Service Properties** die Registerkarte **Security**.
   2. **Akzeptierte Communitynamen**: Für jede Community die Zugriff auf den SNMP-Agenten haben soll, können Zugriffsrechte definiert werden.

      Klicken Sie auf **Add...**, geben Sie eine gültige Community ein (z. B. **public**) und wählen Sie bei **Community rights READ WRITE** für **SNMP GET/SET** Zugriff oder **READ ONLY** für **GET** Zugriff für diese Community.

      Setzen Sie die **Rechte** für die Community auf **LESEN SCHREIBEN** (im Standardfall für **public**).
   3. **SNMP-Pakete von jedem Host annehmen/SNMP-Pakete von diesen Hosts annehmen**: Hier können Sie Server auswählen, von denen SNMP-Pakete akzeptiert werden sollen, oder alle auswählen.

      SNMP wird mit höchster Zugriffssicherheit installiert. Deswegen müssen Sie hier unbedingt die Management-Station eintragen oder die Option **Accept SNMP packets from any host** setzen.

      Da SNMP ein offenes Protokoll ohne Passwortsicherung ist, sollten nur die Management-Stationen eingetragen werden, die auch als solche fungieren sollen. Unbefugte Teilnehmer des Netzes könnten sonst wichtige Parameter des Systems verändern und damit den Server-Betrieb stören.

4. Aktivieren Sie die Option **Send authentication trap**, um dem SNMP Dienst zu erlauben, einen SNMP Trap **authentication failure** zu senden, wenn eine nicht autorisierte Management-Station versucht Zugriff auf diesen Server zu erhalten.
5. Klicken Sie auf **OK**.

   Sie können auf den Link **Learn more about SNMP** klicken, um sich detaillierte Informationen zu den SNMP Konfigurationsoptionen anzeigen zu lassen.

4. SNMP-Dienst starten

   Starten Sie den SNMP-Dienst unter **Services**. Wählen Sie dazu **Start** aus dem Kontextmenü.

2.4.2 Für Environment mit installiertem Server Core

Im lokalen Konsole-Environment des Server Core, ist das GUI-basierte Management-Tool der Microsoft Management-Konsole (MMC) nicht verfügbar. Sie müssen das Management-Tool auf einem anderen Terminal mit Windows 8, Windows 7, Windows Server 2012, Windows Server 2008, oder Windows XP starten und es über Remote verbinden. Die Vorgehensweise wird im Folgenden dargestellt.

Um die Einstellung des SNMP-Services zu konfigurieren, wird ein weiteres Windows Terminal (nicht mit Server Core von Windows Server 2008 installiert) benötigt. Stellen Sie es zuerst bereit.

1. Zur Überprüfung, ob der SNMP-Dienst installiert ist und gestartet wurde, führen Sie auf dem Terminal mit Server Core das folgende Kommando aus:

   ```
   > sc query SNMP
   ```

   Ist der SNMP-Service nicht installiert, führen Sie folgendes Kommando aus, um den SNMP-Service zu installieren.

   ```
   > start /w ocsetup SNMP-SC
   ```

2. Melden Sie sich als Administrator oder als Benutzer mit Administrator-Rechten an.
3. Geben Sie folgende Kommandos nach der Eingabeaufforderung ein.

Für Windows Server 2008, ist die Firewall standardmäßig freigeschaltet. Um die Firewall über Remote zu steuern, muss der Zugriff erlaubt werden.

```
> netsh firewall set service remoteadmin enable
> netsh advfirewall set currentprofile settings
remotemanagement enable
```

Befolgen Sie die folgenden Schritte auf dem anderen Windows Terminal, um Server Core zu verbinden.

4. Starten Sie eine Eingabeaufforderung auf dem anderen Windows Terminal, und führen Sie das folgende Kommando aus. Während der Durchführung werden Sie aufgefordert das Administrator-Passwort einzugeben. Geben Sie die IP-Adresse des überwachenden Servers (Server Core) in "xxx.xxx.xxx.xxx" des folgenden Kommandos ein.

   ```
   net use \\xxx.xxx.xxx.xxx\c$ /u:Administrator
   ```

5. Führen Sie folgendes Kommando aus.

   ```
   >services.msc
   ```

6. Wählen Sie aus dem Menü **Action** die Option **Connect to another computer**.

   Das Fenster **Select Computer** wird geöffnet.

7. Geben Sie die IP-Adresse oder den Computernamen des oben genannten Server Core-Servers bei **Another computer** ein und klicken Sie auf **OK**.

   Die Dienstliste des Server Core-Servers wird angezeigt.

Stellen Sie sicher, dass der SNMP-Service im Service vorkommt.

Im lokalen Konsole-Environment wird weder das Einstellen noch das Ändern des SNMP unterstützt.

3 Installation der ServerView-Agenten

Bei Verwendung einer Public Key-Infrastruktur (PKI) zur Client-Authentifzierung:

Client-Authentifizierung schützt den verwalteten Server sowohl vor dem Zugriff einer nicht vertrauenswürdigen Management-Station als auch vor dem Zugriff einer nicht-privilegierten Anwendung, die auf der Management-Station läuft. Sie können die Zertifikatsdateien entweder gleich zu Beginn mit den ServerView-Agenten installieren oder auf einem verwalteten Server, auf dem die ServerView-Agenten bereits installiert sind.

Bei der Installation der Zertifikatsdateien mit den ServerView-Agenten müssen die Zertifikatsdateien bereits vor den Agenten auf dem verwalteten Server installiert sein.

Nähere Informationen finden Sie im Handbuch "Benutzerverwaltung in ServerView".

Wenn bereits eine neuere Version der ServerView-Agenten installiert ist, können Sie keine Downgrade-Installation durchführen. Zur Durchführung eines Downgrades müssen Sie zunächst alle vorhandenen ServerView-Agenten deinstallieren.

Vor der Installation der ServerView-Agenten für Windows müssen Sie unbedingt die SNMP-Dienste im Betriebssystem installieren und aktivieren. Andernfalls kann die Management-Station die Server nicht überwachen (weitere Informationen finden Sie unter "SNMP-Dienste konfigurieren" auf Seite 30). Außerdem sollten Sie im Vorfeld der Installation das Sicherheitskonzept von ServerView berücksichtigen. Weitere Informationen finden Sie unter "SNMP-Sicherheitskonzept" auf Seite 26.

3.1 Agenten installieren und konfigurieren

Die bedienerlose Installation der ServerView-Agenten wird unter "Installation über die Kommandoschnittstelle" auf Seite 63.

Installieren der ServerView-Agenten für Windows von der ServerView Suite DVD 2:

1. Legen Sie die ServerView Suite DVD 2 in das Laufwerk ein. Wird die DVD nicht automatisch gestartet, dann klicken Sie auf die Datei **start.html** im root-Verzeichnis der DVD.
2. Markieren Sie die Option **ServerView Software Products**.
3. Wählen Sie im angezeigten Fenster die gewünschte Sprache aus.
4. Wählen Sie **ServerView – Agents and Providers**.
5. Starten Sie das entsprechende Programm: **ServerViewAgents_Win_ i386.exe** oder **ServerViewAgents_Win_x64.exe**

Nach dem Starten wird ein Fenster zur Auswahl der Sprache für die Installation angezeigt:

1. Wählen Sie die Sprache aus und klicken Sie auf **OK**.

Wählen Sie die für Sie günstigste Installation.

1. Installieren Sie die Agenten mit den betriebssystemspezifischen Befehlen.
2. Folgen Sie den Anleitungen auf dem Bildschirm.

Startphase des Setup-Wizards

Nach der Bestätigung der Lizenzvereinbarungen überprüft das Setup, ob schon eine ältere Version der ServerView-Agenten auf dem Server installiert ist. In diesem Fall können Sie eine Upgrade-Installation vornehmen. Bei diesem Vorgang wird die aktuelle Konfiguration gespeichert, die alte Version wird gelöscht und die neue Version wird ausgehend von der vorherigen Konfiguration installiert. Sie können in diesem Fall keine Änderungen vornehmen.

Falls noch keine Agenten-Installation vorliegt, wird das folgende Fenster geöffnet:

Fujitsu ServerView Agents - Setup Wizard
Setup Level
Choose your install option
FUJITSU
Typical (High security)
Standard components are installed with highest possible security settings. SNMP sets are generally disabled! Critical and major traps are forwarded to the system eventlog.
Typical (Administrator account based security)
Standard components are installed with password protected security. Only system administrators can do SNMP sets. User name and password are required. Remote system shutdown is enabled! Critical and major traps are forwarded to system eventlog.
Typical (Without any security)
Everyone can do SNMP sets. Remote system shutdown is enabled! Critical and major traps are forwarded to the system eventlog.
Expert (Advanced users)
You can select the components to install and create your personal configuration. Configuration data can be saved to file for later use.
InstallShield
< Back
Next >
Cancel

Bild 2: Fenster **Setup Level**

Das Setup bietet Ihnen vier vordefinierte Modi zur Agenteninstallation:

- Typical (High security)
- Typical (Administrator account based security)
- Typical (Without any security)
- Expert (Advanced users)

Wählen Sie eine der drei Standard-Installationen, so sind keine weiteren Angaben notwendig. In diesen Modi werden die für Operations Manager benötigten SNMP-Agents und die wichtigsten Tools (Configuration, Maintenance, Diagnostic) installiert; siehe dazu "Installierte Tools" auf Seite 56. Hierbei verwendet das Setup jeweils entsprechend der ausgewählten Sicherheitsstufe unterschiedliche Standardwerte.

Der letzte Modus ist der Modus **Expert (Advanced users)**, in dem Sie die Installation und Konfiguration individuell angeben können. Wählen Sie diesen Modus aus, so geben Sie Wizard geführt die gewünschte Installation und Konfiguration an.

Wählen Sie keinen Modus aus, wird **Typical (High security)** als Standard verwendet.

Typical (High security)
Der Standardinstallationsmodus hat die höchste Sicherheitsstufe und erlaubt keine SNMP SET-Operationen. SET-Operationen können auch dann nicht durchgeführt werden, wenn die verwendete SNMP-Community über Schreibrechte verfügt.

Sie können die Standard-Installation nachträglich umkonfigurieren, indem Sie z. B. der Community Schreib/Leserechte zuordnen, Benutzergruppen und Benutzer einrichten, den Agenten entsprechend neu konfigurieren.

Typical (Administrator account based security)
Bei dieser Standard-Installation sind SNMP-SET-Operationen erlaubt. SET-Operationen auf der Management-Station sind passwortgeschützt und beinhalten eine Authentifizierung für lokale Administratoren und Benutzer, lokale Passwörter und Administratorzugriffsrechte. Es besteht jedoch keine Sicherheit für SET-Operationen, die mit anderen SNMP-Tools durchgeführt werden. Die Durchführung von SET-Operationen erfordert Schreibrechte für die verwendete SNMP-Community. Andernfalls wird die SET-Operation durch die Sicherheitsmechanismen des Betriebssystems verhindert.

Sie können die Standard-Installation nachträglich umkonfigurieren, indem Sie z. B. mit betriebssystemspezifischen Mitteln Benutzergruppen und Benutzer einrichten sowie den Agenten mit dem Konfigurationstool **Agenten Konfiguration** entsprechend neu konfigurieren.

Typical (Without any security)
Bei der Standard-Installation ohne irgendwelche Absicherung sind SNMP-SET-Operationen erlaubt und werden ohne weitere Überprüfung zugelassen. Dieser Installationsmodus ist nur sinnvoll für abgesicherte interne Netze. Die Durchführung von SET-Operationen erfordert Schreibrechte für die verwendete

SNMP-Community. Andernfalls wird die SET-Operation durch die Sicherheitsmechanismen des Betriebssystems verhindert.

Expert (Advanced users)
Im Expertenmodus haben Sie folgende Möglichkeit:

- weitere Komponenten auszuwählen
- das Agenten-Paket individuell zu konfigurieren. Sie können die SNMP-Trap-Weiterleitung, die SNMP-Sicherheitseinstellungen sowie das Verhalten beim System-Shutdown individuell konfigurieren.
- den Remote Management-Controller vorkonfigurieren. Sie können schon während der Installation wichtige Einstellungen des Remote Management-Controllers vornehmen und diese während der Installation auf das System übertragen.
- eine Konfigurationsdatei für eine spätere automatische Installation (d.h. unbeaufsichtigtes Setup) erstellen. Sie können Ihre Einstellungen für die Management-Controller-Konfiguration und die Agenten-Konfiguration speichern und bei einer automatischen Installation verwenden.

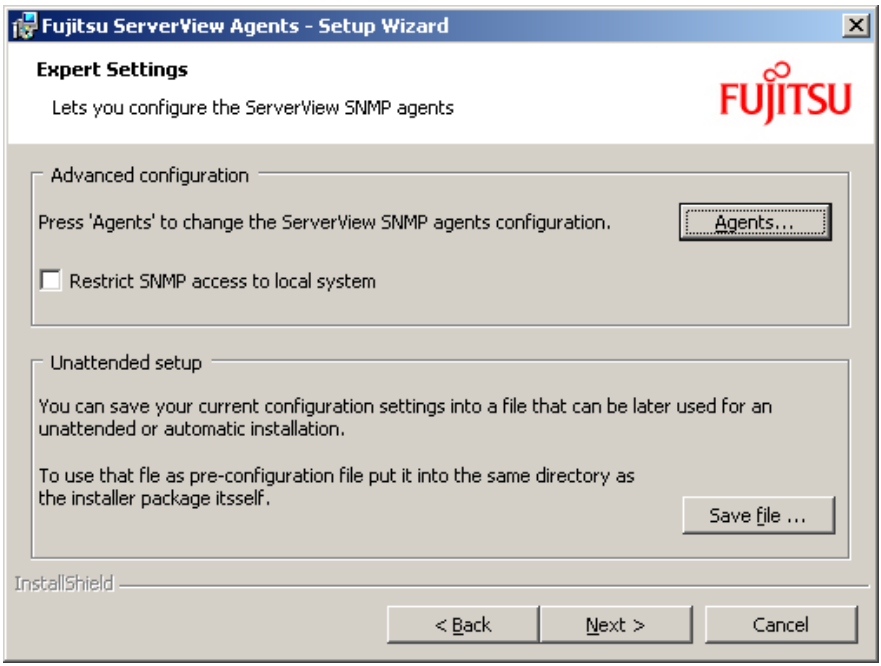

Fujitsu ServerView Agents - Setup Wizard
Expert Settings
Lets you configure the ServerView SNMP agents
FUJITSU
Advanced configuration
Press 'Agents' to change the ServerView SNMP agents configuration.
Agents...
Restrict SNMP access to local system
Unattended setup
You can save your current configuration settings into a file that can be later used for an unattended or automatic installation.
To use that file as pre-configuration file put it into the same directory as the installer package itsself.
Save file ...
InstallShield
< Back
Next >
Cancel

Bild 3: Fenster **Expert Settings**

Agents ...

Öffnet ein Fenster, in dem Sie die Konfiguration der ServerView-Agenten vornehmen. Näheres dazu entnehmen Sie dem folgenden Abschnitt.

Restrict SNMP access to local system

Diese Option setzt in den SNMP-Einstellungen den Wert **Restrict access to these host only** und trägt den LOOPBACK-Adapter ein. In diesem Fall kann von außerhalb nicht auf das System zugegriffen werden. Diese Option ist sinnvoll, falls der Event Manager auf dem Server installiert ist und der Server nicht als Management-Station genutzt wird.

Save file ...

Öffnet ein Fenster, in dem Sie den Pfad zur Speicherung der Konfigurationsdatei **Setup.pre** eingeben können.

Diese Datei wird für automatische Installationen (unbeaufsichtigte Setups) verwendet (siehe auch "Installation über die Kommandoschnittstelle" auf Seite 63).

Die Konfigurationsdatei muss im gleichen Verzeichnis liegen wie die **Setup.exe**.

<Back

Kehrt zum vorherigen Fenster zurück.

Next>

Zeigt das nächste Fenster an.

Cancel

Beendet die Installation.

Aufgrund von Änderungen an der Architektur kann beim Setup-Wizard das Tool zur Systemkonfiguration nicht mehr (über die Schaltfläche **System ...**) gestartet werden. Um die Systemeinstellungen zu konfigurieren, beenden Sie das Agenten-Setup und starten Sie das Dienstprogramm zur Systemkonfiguration (siehe "Server konfigurieren" auf Seite 23).

Konfiguration der ServerView-Agenten

Klicken Sie die Schaltfläche **Agents ...** an, um die ServerView-Agenten zu konfigurieren. Das Fenster **ServerView SNMP agents settings (offline)** wird geöffnet.

Dieses Fenster enthält folgende Registerkarten:

- Registerkarte **Trap Forwarding**
- Registerkarte **System Shutdown**
- Registerkarte **Security Settings**
- Registerkarte **Threshold Monitoring**

Registerkarte Trap Forwarding
Alle SNMP-Traps, die von den ServerView-Agenten erzeugt werden, können optional in die System-Ereignisanzeige oder als Administrator-Meldung weitergeleitet werden. Die Weiterleitung hängt von dem Schweregrad ab, der dem Trap zugewiesen wurde. Es stehen folgende Schweregrade zur Auswahl:

- critical (kritische Traps)
- major (wichtige Traps)
- minor (weniger wichtige Traps)
- informational (informative Traps)

Die Abbildung der Gewichtung auf den Typ der Ereignisanzeige erfolgt folgendermaßen:

Trap-Gewichtung	**Typ in der Ereignisanzeige**
Critical and major traps	Fehler
Minor traps	Warnung
Informational traps	Information

Für eine Weiterleitung der Traps an den Administrator muss der Nachrichtendienst auf dem Server konfiguriert und gestartet sein. Außerdem müssen die Ziele für die Meldungen in den Eigenschaften des Windows Server Manager konfiguriert werden.

Der Quellname für die von ServerView-Agenten berichteten Ereignisse ist **ServerView Agents**. ServerView-Agenten senden Berichte an das Anwendungsprotokoll.

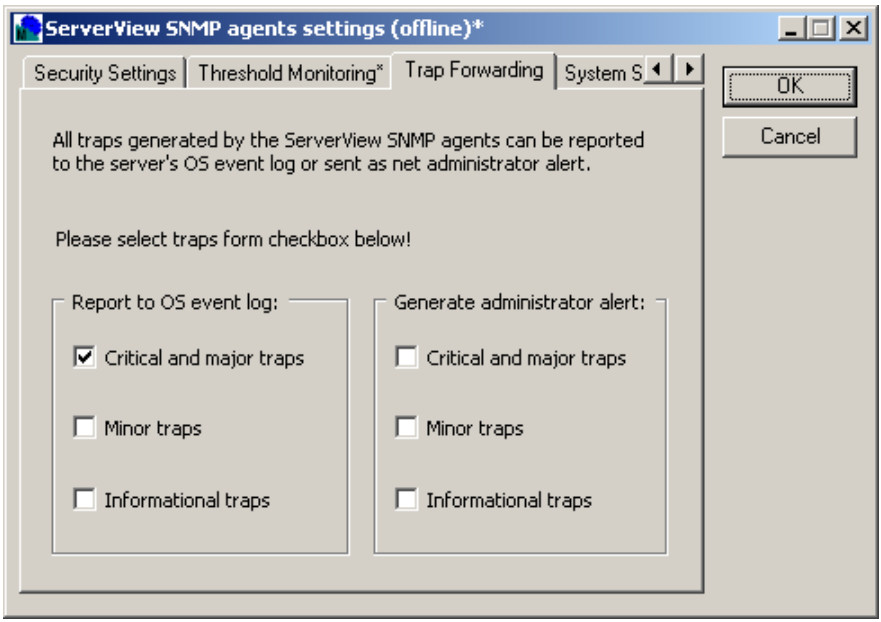

ServerView SNMP agents settings (offline)*
Security Settings
Threshold Monitoring*
Trap Forwarding
System S
OK
Cancel
All traps generated by the ServerView SNMP agents can be reported to the server's OS event log or sent as net administrator alert.
Please select traps form checkbox below!
Report to OS event log:
Critical and major traps
Minor traps
Informational traps
Generate administrator alert:
Critical and major traps
Minor traps
Informational traps

Bild 4: Registerkarte **Trap Forwarding**

Auf der Registerkarte **Trap Forwarding** können Sie auswählen, welche Typen von SNMP-Traps weitergeleitet werden. Standardmäßig werden die kritischen und die wichtigen Traps an die System-Ereignisanzeige weitergeleitet.

Registerkarte System Shutdown

Die ServerView-Agenten können einen System-Shutdown initiieren. Der Shutdown kann durch eine Operation an der Management-Station oder durch Auftreten eines Fehlers im System ausgelöst werden.

Die ServerView-Agenten starten zuerst immer einen Soft-Shutdown, d.h. der Anwender wird aufgefordert, seine Anwendungen zu beenden und den Shutdown explizit auszulösen. Nach Ablauf eines voreingestellten Zeitraums initiieren die ServerView-Agenten ein "hartes" Herunterfahren. Hierbei wird das Betriebssystem auch dann heruntergefahren, wenn das Herunterfahren nicht ausdrücklich bestätigt wurde und nicht alle Daten auf der Festplatte gespeichert wurden. Als Default-Wert sind 120 Sekunden vorgegeben. Der Wert für diese Zeitspanne sollte entsprechend hoch gesetzt werden, wenn große Datenmengen auf die Platte zurückgeschrieben werden müssen.

Zusätzlich kann eine Anwendung (ein Shutdown-Job) gestartet werden, bevor der Soft-Shutdown initiiert wird.

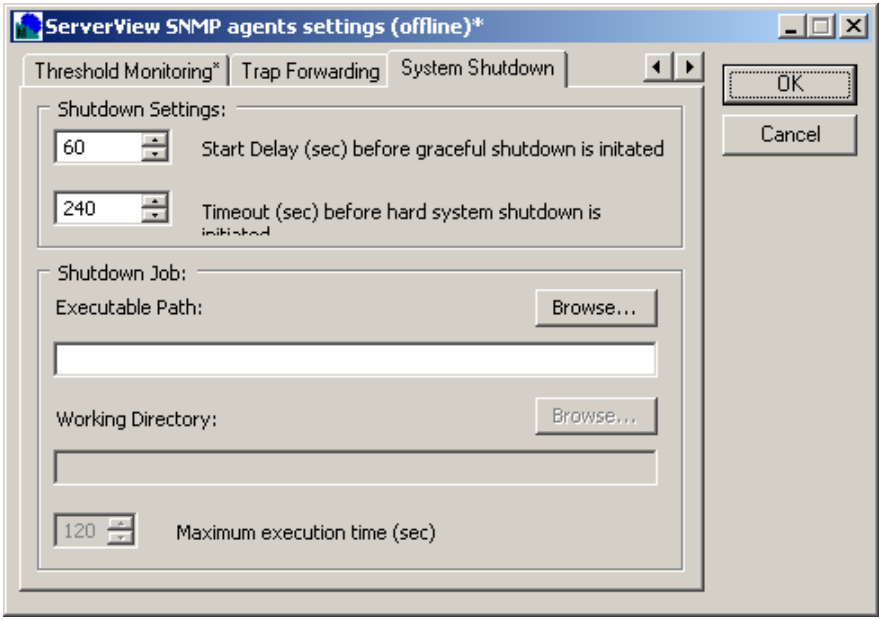


Bild 5: Registerkarte **System Shutdown**

Auf der Registerkarte **System Shutdown** können Sie die folgenden Einstellungen für das Herunterfahren festlegen:

Start Delay (sec)
Gibt die Verzögerung in Sekunden an, bevor der Shutdown gestartet wird. Innerhalb dieser Zeit lässt sich der Shutdown noch an der System-Konsole abbrechen.

Timeout (sec)
Gibt die Zeitspanne in Sekunden an, in welcher der Shutdown mit Datensicherung (Soft-Shutdown) vollzogen sein muss. Wird diese Zeitspanne überschritten, so wird ein Shutdown ohne Datensicherung (Hard-Shutdown) gestartet.

Executable Path
Pfadname eines ausführbaren Programms oder Skripts. Der Pfad kann auch Umgebungsvariablen enthalten, z. B. **%SystemRoot%**.

Working Directory
Gibt das Arbeitsverzeichnis für die Anwendung an.

Maximum execution time (sec)
Gibt die maximale Dauer der Anwendung an. Nach Ablauf der eingestellten Maximalzeit wird der Shutdown fortgesetzt.

Registerkarte Security Settings
Die ServerView-Agenten bieten in Verbindung mit der Management-Station ein erweitertes Sicherheitskonzept, um SNMP-SET-Operationen auf dem Server einzuschränken. Es besteht die Möglichkeit, SET-Operationen generell zu verbieten oder in Verbindung mit der Management-Station durch eine Benutzer-Authentifizierung zu schützen.

Ist die Benutzer-Authentifizierung aktiviert, so wird vor jeder Ausführung einer SET-Operation eine Benutzer-Authentifizierung durchgeführt. Verläuft diese erfolgreich, so wird zusätzlich die Zugehörigkeit zu einer vom Administrator vergebenen Benutzergruppe überprüft.

Die Benutzer-Authentifizierung funktioniert nur mit dem Operations Manager auf der Management-Station. Es ist für andere SNMP-Tools wirkungslos.

Sie können die Konfiguration der Sicherheitseinstellungen auf der folgenden Registerkarte vornehmen:

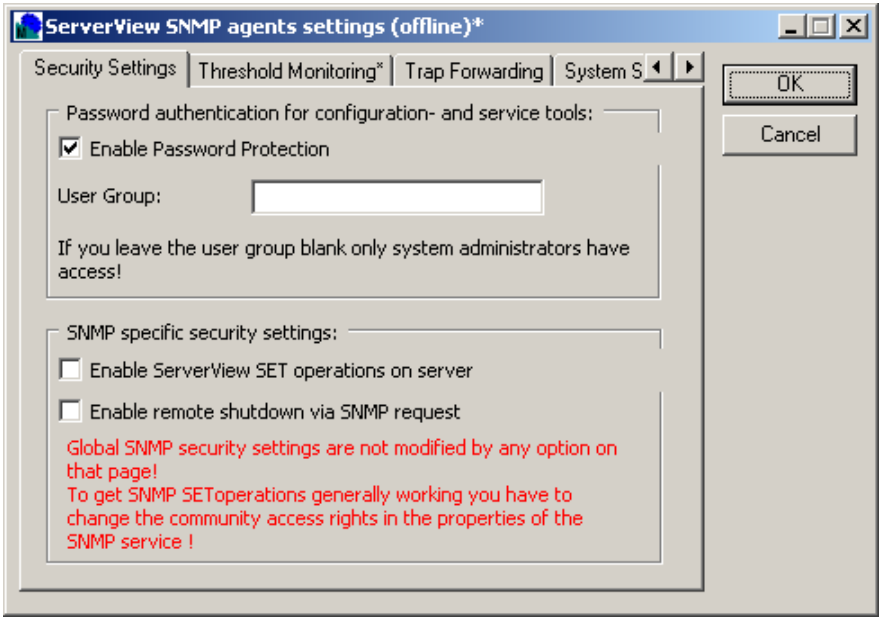

ServerView SNMP agents settings (offline)*
Security Settings
Threshold Monitoring*
Trap Forwarding
System S
OK
Cancel
Password authentication for configuration- and service tools:
Enable Password Protection
User Group:
If you leave the user group blank only system administrators have access!
SNMP specific security settings:
Enable ServerView SET operations on server
Enable remote shutdown via SNMP request
Global SNMP security settings are not modified by any option on that page!
To get SNMP SEToperations generally working you have to change the community access rights in the properties of the SNMP service !

Bild 6: Registerkarte **Security Settings**

Enable Password Protection

Schaltet die Benutzer-Authentifizierung für SNMP-SET-Operationen ein bzw. aus.

User Group

Gibt die Benutzergruppe an, zu der die Benutzer gehören müssen, die SET-Operationen auf dem Server ausführen dürfen. Sie können hier eine beliebige Benutzergruppe anlegen.

Falls die Benutzergruppe noch nicht existiert, so müssen Sie die Benutzergruppe auf dem Server mit betriebssystemspezifischen Mitteln nachträglich noch anlegen.

An dieser Stelle wird aber der Benutzergruppe kein Benutzer zugeordnet. Warten Sie bis später. Die Zuweisung eines Benutzers zu einer Benutzergruppe auf der Betriebssystemebene erfolgt vor oder nach der

Installation des Agenten. Aus Sicherheitsgründen ist es sinnvoll, nur einen Benutzer einzutragen.

Geben Sie für **User Group** keinen Namen an, so dürfen nur lokale System-Administratoren SET-Operationen auf dem Server ausführen.

Wenn Sie die ServerView Agenten mit dem ServerView Installation Manager installieren, wird die **User Group**auf "FUJITSU SVUSER" gesetzt.

Enable ServerView SET operations on server

Erlaubt SNMP-SET-Operationen für die ServerView-Agenten. Verbieten Sie SET-Operationen, so werden alle SNMP-SETs generell abgewiesen, unabhängig davon, mit welchem Tool der SET durchgeführt wird.

Diese Option gilt nur für ServerView-Agenten. SET-Operationen für andere SNMP-Agenten werden davon nicht beeinflusst.

Enable remote shutdown via SNMP request

Einige SET-Operationen bewirken einen Shutdown oder Neustart des Systems. Hier können Sie diese speziellen SET-Operationen zulassen oder verbieten.

Registerkarte Threshold Monitoring

Über die Registerkarte **Threshold Monitoring** können Sie die Schwellwertüberwachung für Threshold Manager aktivieren oder deaktivieren.

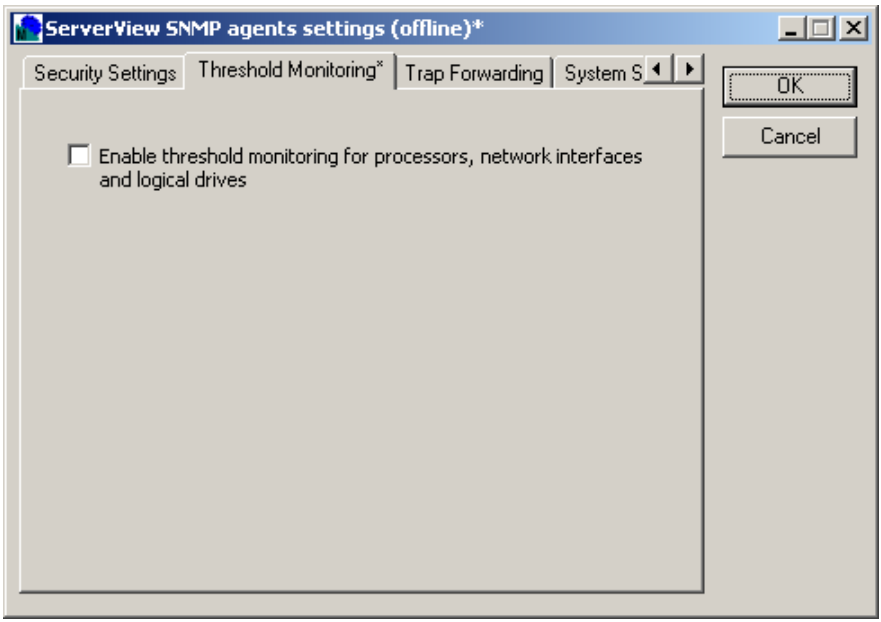


Bild 7: Registerkarte **Threshold Monitoring**

Zielordner auswählen

Klicken Sie im Fenster **Expert Settings** auf **OK**, um die Agenten-Konfigurationen zu bestätigen. Wechseln Sie dann zum Fenster **Destination Folder**, um den gewünschten Installationsordner auszuwählen.

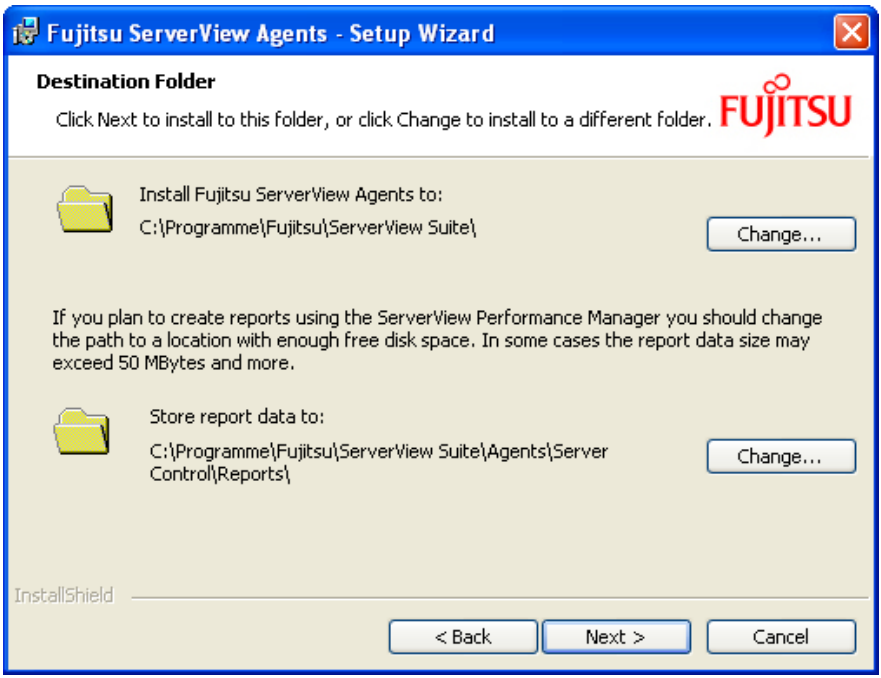

Fujitsu ServerView Agents - Setup Wizard
Destination Folder
Click Next to install to this folder, or click Change to install to a different folder.
FUJITSU
Install Fujitsu ServerView Agents to:
C:\Programme\Fujitsu\ServerView Suite\
Change...
If you plan to create reports using the ServerView Performance Manager you should change the path to a location with enough free disk space. In some cases the report data size may exceed 50 MBytes and more.
Store report data to:
C:\Programme\Fujitsu\ServerView Suite\Agents\Server Control\Reports\
Change...
InstallShield
< Back
Next >
Cancel

Bild 8: Fenster **Destination Folder**

Der ServerView-Agent wird standardmäßig im Installationsverzeichnis installiert. Mit der Schaltfläche **Change...** können Sie den Ordner wechseln.

Bei Verwendung des Performance Managers werden Reportdaten standardmäßig im Installationsverzeichnis abgelegt. Diese können jedoch, je nach Anwendungsfall, leicht 50 MByte und mehr belegen. Sie haben deshalb die Möglichkeit, über die Schaltfläche **Change...** ein anderes Verzeichnis mit genügend Platz auszuwählen.

Installationsumfang festlegen (Setup Type)

Klicken Sie im Fenster **Expert Settings** auf **OK**, um die Agenten-Konfigurationen zu bestätigen. Öffnen Sie anschließend das Fenster **Setup Type** und wählen Sie den Setup-Typ aus.

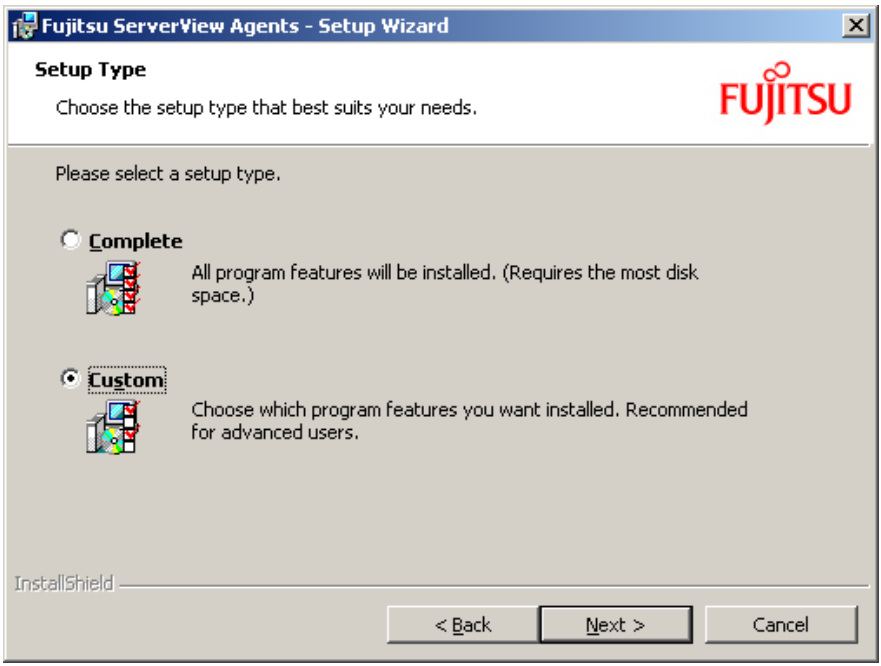

Fujitsu ServerView Agents - Setup Wizard
Setup Type
Choose the setup type that best suits your needs.
FUJITSU
Please select a setup type.
Complete
All program features will be installed. (Requires the most disk space.)
Custom
Choose which program features you want installed. Recommended for advanced users.
InstallShield
< Back
Next >
Cancel

Bild 9: Fenster **Setup Type**

Sie können den Installationsumfang auswählen.

Complete

Startet eine Installation, bei der alle Komponenten installiert werden. Sie benötigt den meisten Speicherplatz.

Custom

Bietet die Möglichkeit an, einzelne Komponenten auszuwählen. Zusätzlich können Sie den Speicherort für die Reportdaten und den Port für den **ServerView Remote Connector** Dienst festlegen.

Wenn Sie **Custom** und dann **Next** auswählen, wird das folgende Fenster geöffnet:

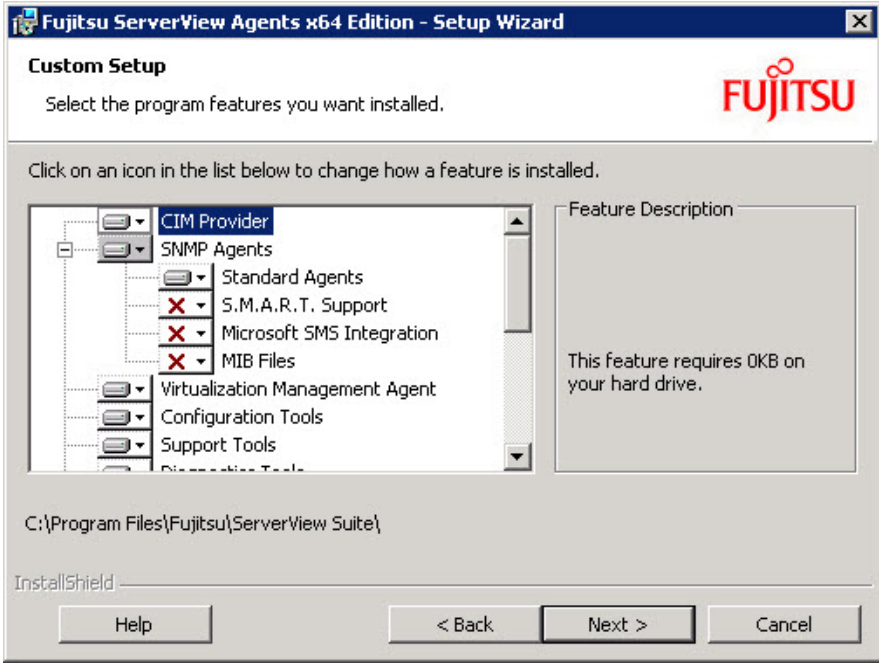


Bild 10: Fenster **Custom Setup**

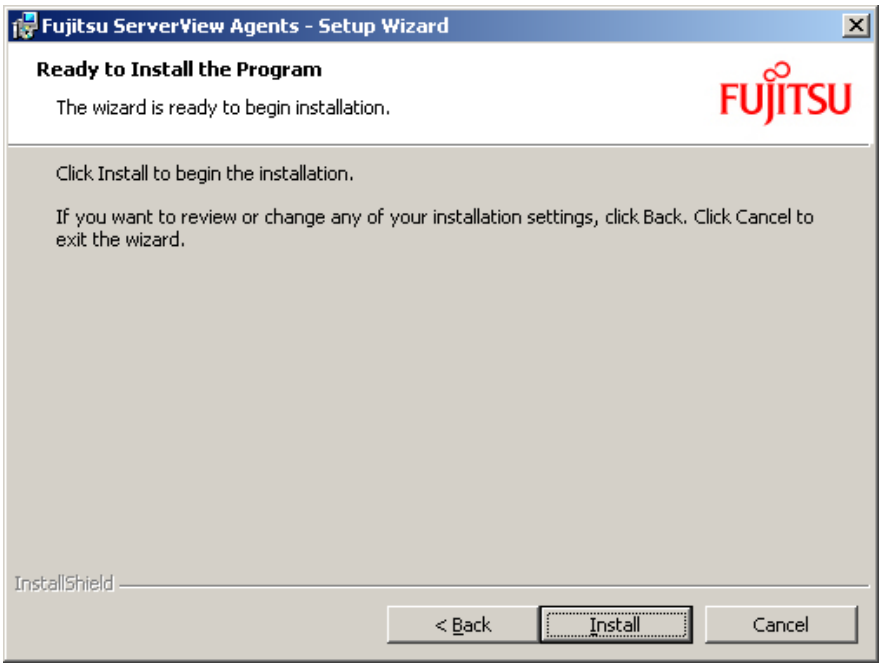
Sie haben folgende Wahlmöglichkeiten:

Funktion	Beschreibung
Standard Agents	ServerView-Agenten, die zwingend notwendig sind für den Operations Manager
S.M.A.R.T. Support	Unterstützung des S.M.A.R.T. Ereignis-Monitoring
Microsoft SMS Integration	Software für die automatische MIF-Datei-Erzeugung für Microsoft SMS V 1.2 und V 2.0
MIB Files	ServerView-MIB-Dateien

Funktion	Beschreibung
Configuration Tools	Tools zur Agenten- und System-Konfiguration
Support Tools	Werkzeuge für den Servicetechniker
Diagnostics Tools	Verschiedene Diagnose-Tools (z. B. zur Überprüfung der Installation), dienen nur zur Support-Unterstützung
System Monitor Web-Oberfläche	Tool zur Systemüberwachung (Web-basiert).
System Monitor	Tool zur Systemüberwachung (lokales Tool).
Windows Management Integration	Integration in das Microsoft Windows Management Instrumentation (WMI)
Virtualization Management Agent	Stellt Leistungsdaten für virtuelle Maschinen (Xen, Hyper-V, VMware) bereit.
HP Systems Integration	Integration in HP SIM (System Insight Manager)
Asset CLI	Tool zur lokalen Ermittlung von Systemdaten auf PRIMERGY Servern.
PrimeCollect	Tool zum Sammeln und Speichern von Informationen über die Hard- und Software von PRIMERGY Servern.
Help Files	Hilfedateien
Remote Connector Service	Bietet HTTP-basierte Dienste an.
Server Control Service	Erforderlicher Basis-Service

Funktion	Beschreibung
CIM-Provider	Wird das Betriebssystem von CIM Provider nicht unterstützt, so wird das Feature "ServerView CIM Provider" im Schritt **Custom Setup** nicht angeboten. Installiert die ServerView CIM Provider, um eine Verwaltung der PRIMERGY Server über die CIM-Infrastruktur zu ermöglichen. Siehe dazu auch das Benutzerhandbuch "ServerView CIM Providers for the management of PRIMERGY servers".

Nach der Auswahl der Komponenten wird folgendes Fenster angezeigt:


Fujitsu ServerView Agents - Setup Wizard
Ready to Install the Program
The wizard is ready to begin installation.
FUJITSU
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel

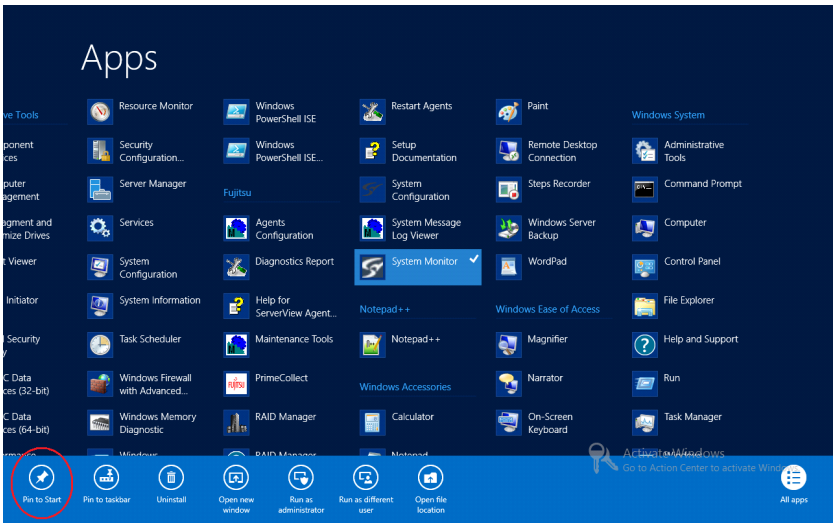
Klicken Sie auf **Install**, um den Installationsvorgang zu starten.

3.2 Installierte Tools

- Unter Windows Server 2008: Nach erfolgreicher Installation stehen verschiedene Tools zur Verfügung unter:

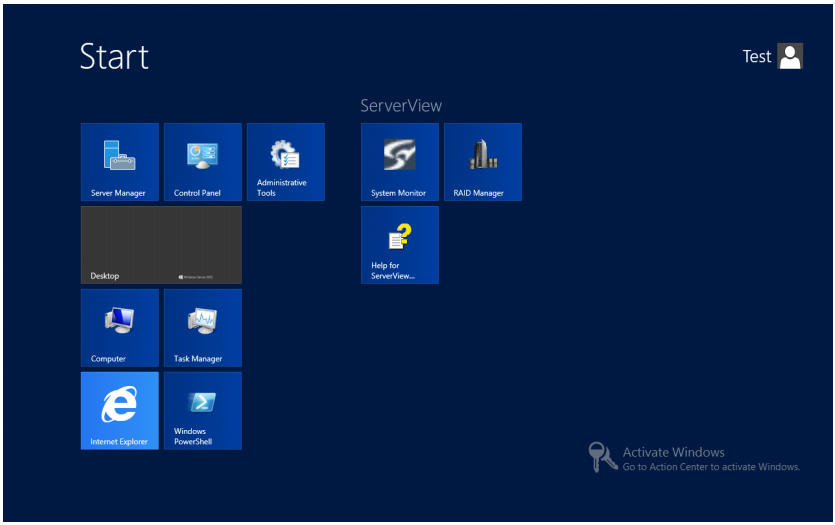
  Start – **Programs** – **Fujitsu** – **ServerView Suite** – **Agents**

- Unter Windows Server 2012: Nach erfolgreicher Installation stehen verschiedene Tools auf der Seite **Apps** zur Verfügung. Über das Symbol **Pin to Start** können Sie Anwendungen auf die **Start**-Seite verschieben.



Auf der **Start**-Seite können Sie Anwendungsgruppen erstellen. Wählen Sie die relevanten Anwendungen aus und klicken Sie unten rechts auf das Minuszeichen.

Daraufhin wird ein Dialogfeld geöffnet, in dem Sie einen Namen für die Gruppe eingeben können. Die neue Gruppe wird auf der **Start**-Seite angezeigt, z. B. Gruppe **ServerView**.



Nach der Installation dauert es einige Zeit, bis die Konfiguration vollständig angezeigt wird. Deshalb kann es sein, dass Sie bei der Abfrage der Konfiguration noch nicht alle Werte bekommen.

Wartungs-Tools

CPU-Status	Zeigt eine Übersicht der vorhandenen CPUs.
Hauptspeicher-Status	Bietet eine detaillierte Liste aller installierten Speichermodule. Hier können Sie den Fehlerzähler für eines oder mehrere Module zurücksetzen. Ein Hauptspeicher-Status ist sinnvoll, nachdem Sie ein Speichermodul ausgetauscht haben.
*) Zähler	Setzt die Zähler (Gesamteinschaltdauer, Gesamtausschaltdauer und Gesamtanzahl der Einschaltvorgänge des Systems) auf Null zurück. Das ist sinnvoll, nachdem Sie die CMOS-Batterie ausgetauscht haben.

*) Nur für PRIMERGY

Menü Diagnose

Diagnose Report	Untersucht die Installation der ServerView-Komponenten auf dem Server.
Agenten Neustart	Startet die ServerView-Agenten neu.
*) Fehlerspeicheranzeige	Gibt die Fehlermeldungen des Service Prozessors aus.

*) Nur für PRIMERGY

PrimeCollect
Tool zum Sammeln und Speichern von Informationen über die Hard- und Software von PRIMERGY Servern.

Agenten Konfiguration
Ermöglicht die nachträgliche Konfiguration der ServerView-Agenten.

System Konfiguration
Ermöglicht die nachträgliche Konfiguration der Server Firmware.

System Monitor Web-Oberfläche/System Monitor
Über diesen Eintrag starten Sie die ServerView System Monitor Web-Oberfläche oder den lokalen ServerView System Monitor. Über ServerView System Monitor können Sie folgende Serverinformationen lokal auf Ihrem Server überwachen und überprüfen:

- Informationen über die Umgebung, inklusive Lüfter und Temperatursensor
- Informationen über die Stromversorgung
- Informationen zu den Festplatten. Diese Informationen sind nur verfügbar, wenn ServerView RAID Manager auf dem System installiert ist.
- Informationen über die Systembaugruppe
- Informationen über das Netzwerk
- Informationen über den Driver Monitor
- Informationen über den Update-Status
- Der Inhalt des System Event Log (SEL) (nur bei der ServerView System Monitor Web-Oberfläche)

Eine Beschreibung von System Monitor finden Sie im Benutzerhandbuch "ServerView System Monitor".

3.3 RAID konfigurieren

Zur RAID-Konfiguration können Sie den ServerView RAID Manager verwenden, den Sie auf der ServerView Suite DVD unter **RAID Manager** finden.

3.4 APC- und Masterguard-USV konfigurieren

Die folgende Beschreibung ist nur gültig für PRIMERGY.

Die Konfiguration der am System oder am Beistellschrank angeschlossenen unterbrechungsfreien Stromversorgungen ist Voraussetzung

- für die Darstellung der USV im Operations Manager,
- zur Einbindung des aktuellen USV-Status.

Zur Ermittlung des USV-Status muss ein USV-SNMP-Agent auf dem Server installiert sein. Der SNMP-Agent wird Ihnen vom USV-Hersteller geliefert. Bei einer USV mit Web-Karte ist der entsprechende SNMP-Agent auf der Web-Karte vorinstalliert.

Zur Kommunikation mit dem USV-SNMP-Agenten benötigt der Operations Manager folgende Daten:

- Hersteller
- Modellbezeichnung
- Basis-OID (object identifier) des SNMP-Agenten
- Name oder IP-Adresse des Hosts

Die IP-Adresse ist zwingend für die SNMP-Kommunikation mit dem Agenten notwendig. Sie geben hier die IP-Adresse des Servers bzw. der USV an.

Für die USV-Modelle von APC und Masterguard ist die Vergabe der Basis-OID für den SNMP-Agenten nicht zwingend erforderlich. Diese beiden Modelle werden anhand des Modell- und Herstellernamens vom Operations Managers erkannt und dieser ordnet die richtigen SNMP OIDs automatisch zu. Es ist empfehlenswert, für diese Typen die Werte aus den angebotenen Voreinstellungen zu übernehmen und nur noch die IP-Adresse zu ergänzen.

UPS-Anwendungen installieren

Um die bestehende USV-Konfiguration in ServerView/Operations Manager anzuzeigen, installieren Sie auf der Management-Station zunächst die Anwendung **PowerChuteBusiness Edition** (für APC-USV mit seriellem Anschluss) oder **upsmon** (für Masterguard-USV).

Bei der Installation werden in der Registry entsprechende Einträge vorgenommen (siehe hierzu auch den Abschnitt zur APC-USV im Operations Manager-Benutzerhandbuch).

Die **PowerChuteBusiness Edition** ist auf der APC CD verfügbar. **upsmon** ist ein eigenständiges Produkt.

USV-Konfiguration unter Windows Server 2008/2012

Über das Menü **Start** können Sie eine USV lokal auf verwalteten Windows-basierten Servern konfigurieren.

1. Windows Server 2008: Wählen Sie auf dem verwalteten Server Folgendes:

   Start – **Programme** – **Fujitsu** – **ServerView Suite** – **Agents** – **System Configuration**

   Windows Server 2012: auf dem verwalteten Server über die **Start**-Seite.

   Es gibt verschiedene Arten, die Konfiguration zu starten. Eine Möglichkeit besteht im Wechseln zur Seite **Apps**. Zum Öffnen dieser Seite klicken Sie auf der **Start**-Seite auf die rechte obere oder untere Ecke. Wählen Sie im angezeigten Fenster die Option **Search**.
2. Wählen Sie auf der Startseite **System Configuration** die Funktionen und klicken Sie auf **Go...**.

3. Wählen Sie in der Baumstruktur **UPS Integration**.

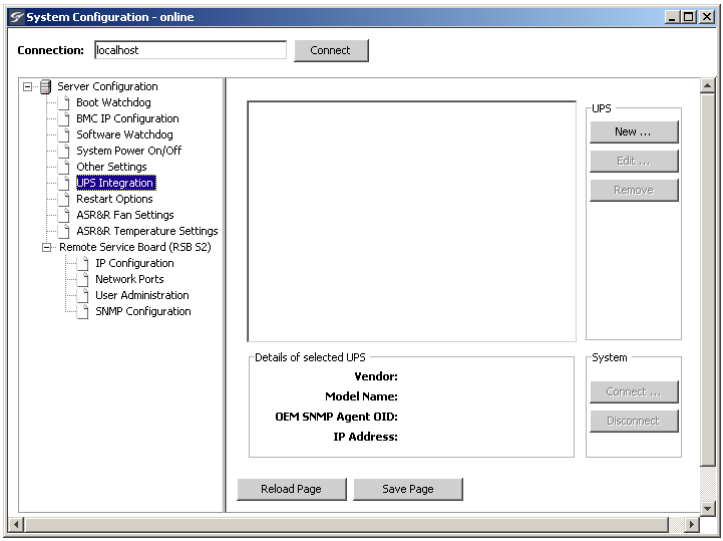


Bild 11: **UPS Integration**

Einzelheiten zu den Parametern finden Sie in der Online-Hilfe von Server Configuration Manager.

Um die Online-Hilfe zu öffnen, gehen Sie folgendermaßen vor:

1. Klicken Sie in den Anzeigebereich, in dem dieser Dialog angezeigt wird.
2. Drücken Sie die Taste **F1**.

3.5 Installation über die Kommandoschnittstelle

Sie können die ServerView-Agenten für Windows über einen Aufruf von Kommandozeilenebene installieren. Der Operations Manager ermöglicht Ihnen dabei auch eine bedienerlose Installation der Agenten. Mit Hilfe der bedienerlosen Installation können Sie Software-Verteilungssysteme wie zum Beispiel Microsoft System Management Server (SMS) Software automatisch verteilen. Die einfachste Form der Software-Verteilung ist die bedienerlose Ausführung des Setups mit der Standardkonfiguration. Sie haben aber die Möglichkeit, die Installation mit Hilfe von Umgebungsvariablen an Ihre Bedürfnisse anzupassen.

Das Setup für die ServerView-Agenten basiert auf der Microsoft Windows Installer-Technologie. Die Setup-Daten befinden sich in der Installer-Datenbank **ServerView Agents.msi**. Die Setup-Daten sind in **Data1.cab** enthalten.

Kommandosyntax von Setup.exe
Wechseln Sie auf die Kommandozeilenebene und rufen Sie auf der obersten Ebene des Installationsverzeichnisses das **setup**-Kommando auf:

```
Setup.exe [/x] | [[/a][/s][/V]]
```

Die Optionen haben dabei folgende Bedeutung:

/x

(Uninstalled mode)

Das Setup deinstalliert das Produkt.

/a

(Administrative mode)

Das Setup wird im Administrator Modus ausgeführt. In diesem Modus werden alle Dateien extrahiert und in ein Verzeichnis installiert. Es werden keine Registry-Einträge oder Verknüpfungen angelegt.

/s

(Silent mode)

Unterdrückt alle Ausgaben auf dem Bildschirm. Die Installation erfolgt komplett im Hintergrund.

/V

(Microsoft Installer Option)

Erlaubt die Übergabe von Argumenten direkt an den Microsoft Installer (MSIEXEC.EXE).

Microsoft Installationseigenschaften

Sie können die Installation durch das Angeben von Eigenschaften beeinflussen. Der Name der Eigenschaft wird immer großgeschrieben. Bei den Werten wird zwischen der Groß- und Kleinschreibung unterschieden.

INSTALLDIR

Setzt das Standard-Installationsverzeichnis neu.

Gültige Pfadnamen, z. B.:

INSTALLDIR=C:\Programs\Fujitsu\ServerView Suite\ServerView agents

Standard: Programmordner des Systems

REBOOT

Beeinflusst das Verhalten bei einem Neustart des Systems nach der Installation. Diese Option verhindert beispielsweise den Neustart des Systems nach einer automatischen Installation für den Fall, dass Komponenten erst nach einem Neustart des Systems ausgetauscht werden können. Mögliche Werte:

F

Es wird immer ein Neustart des Systems durchgeführt.

R

Es wird kein Neustart des Systems durchgeführt.

SETUP_LEVEL

Setzt den Setup-Modus für die Installation. Mögliche Werte:

LevelHigh

(Standard)

Installiert im Setup-Modus **Typical (High Security)**.

Die Installation mit höchster Sicherheitsstufe lässt keine SNMP-Set-Operationen zu.

LevelAdmin

Installiert im Setup-Modus **Typical (Administator account based security)**.

ServerView SNMP-Set-Operationen werden auf lokale Administratorrechte und Passwort geprüft.

LevelAll

Installiert im Setup-Modus **Typical (Without any Security)**.

ServerView SNMP-Set-Operationen werden ohne Überprüfung zugelassen. Dieser Installationsmodus ist nur für abgesicherte interne Netze sinnvoll.

LevelUser

Installiert im Setup-Modus **Expert (Advanced users)**.

ADDLOCAL

Gibt an, welche Module installiert werden sollen. Geben Sie keine Auswahl an, so wird eine Standard-Auswahl installiert. Wollen Sie eine individuelle Auswahl treffen, so müssen Sie die gewünschten Module mit der Variablen **ADDLOCAL** angeben. Die Modulnamen werden durch ein Komma getrennt aufgelistet. Mögliche Werte:

All

Installiert alle Module.

ServerControl

(Standard, muss immer installiert werden)

Installiert den ServerView Base Service.

SnmpAgents

(Standard)

Installiert die ServerView-Agenten.

MIBFiles

Installiert die ServerView-Agenten MIB-Dateien.

SmartSupport

(Standard)

Installiert den ServerView S.M.A.R.T.-Support.

Konfiguration
(Standard)

Installiert die ServerView Konfigurations-Tools.

Diagnose
(Standard)

Installiert die ServerView Diagnose-Tools.

Maintenance
(Standard)

Installiert die Support-Tools.

SMS
Installiert die ServerView Integration in SMS.

WMI
Installiert die ServerView-Integration in SMS.

WCS
Installiert den ServerView Remote Connector.

AssetCLI
Installiert das Tool ServerView Asset CLI.

OnlineDiagnostic
Installiert das Online Diagnose Tool.

PrimeCollect
Installiert das Tool PrimeCollect.

Help
ServerView Hilfedateien.

SSM
Installiert den ServerView System Monitor (lokal) zur Systemüberwachung.

SSMWeb
(Standard)

Installiert die ServerView System Monitor Web-Oberfläche zur Systemüberwachung.

CIM

Installiert den ServerView CIM Provider.

HPSIM

Installiert die ServerView-Integration in HP SIM (HP Systems Insight Manager).

Beispiel

```
ADDLOCAL=ServerControl,MIBFiles,WMI
```

Die Programm-Module ServerView Base Service, ServerView-Agenten MIB-Dateien und ServerView Integration in WMI werden installiert.

Installation mit einer Konfigurationsdatei

Um eine Konfigurationsdatei einzurichten, gehen Sie wie folgt vor:

1. Starten Sie den Setup-Wizard.
2. Wählen Sie den Modus **Expert (Advanced users)**.
3. Konfigurieren Sie im Fenster **Expert Settings** über die Schaltfläche **Agents...** die Einstellungen für die Agenten.
4. Klicken Sie auf die Schaltfläche **Save file ...**, um das Verzeichnis auszuwählen, in dem die Konfigurationsdatei **Setup.pre** gespeichert werden soll. Die Konfigurationsdatei muss in dem gleichen Verzeichnis wie die Microsoft Installer Datenbank (**ServerView Agents.msi**) abgelegt werden.

Bei einem **Setup.exe**-Aufruf werden die Konfigurationsdaten aus der Datei auf das System übertragen, unabhängig davon, welchen Setup-Modus Sie gewählt haben.

Beispiele für Setup.exe

```
Setup.exe /s/V"/qn"
```

Automatische Installation der Standardkonfiguration. Der Setup-Modus ist **Typical (High Security)**, d.h. es sind keine SNMP-SET-Operationen erlaubt und kritische Traps werden in das Systemprotokoll aufgenommen.

Der Installationspfad ist der Programm-Ordner des Systems (z. B. **C:\Programs**).

Folgende Module werden installiert:

- ServerView Base Service
- ServerView-Agenten
- ServerView Konfigurations-Tools
- ServerView Diagnose-Tools
- ServerView Maintenance Tools
- ServerView Remote Connector
- ServerView PrimeCollect

```
Setup.exe /s/V"/qn SETUP_LEVEL=LevelAll
INSTALLDIR="C:\My Programs"
```

Angepasste automatische Installation im Setup-Modus **Typical (Without any security)** und geändertem Installationspfad.

```
Setup.exe /s/V"/qn ADDLOCAL=ServerControl,WMI
INSTALLDIR="C:\My Programs"
```

Automatische Installation der Basis für die Integration in das Windows Management Instrumentation (WMI) mit geändertem Installationspfad.

```
Setup.exe /s/V"/qn ADDLOCAL=ServerControl,WMI
Reboot=R"
```

Automatische Minimal-Installation für die Integration in das Windows Management Instrumentation (WMI) ohne System-Neustart.

3.6 Einstellungen nach der Installation

Nehmen Sie nach der Installation der ServerView-Agenten oder der CIM Provider für Windows folgende Einstellungen vor, um zu gewährleisten, dass der Agent ordnungsgemäß agiert.

3.6.1 Administrativen Benutzer festlegen

Nur die Benutzer, die der Gruppe (**FUJITSU SVUSER**) mit Administrator-Berechtigungen für ServerView angehören, können solche Tätigkeiten durchführen, wie Einstellungen zu Automatic Server Reconfiguration & Restart (ASR) (z.B. für Lüfter, Temperatur, Neustart) für die überwachten Server zu

konfigurieren und die Server vom ServerView Operations Manager aus herunterzufahren. Zu diesem Zeitpunkt muss der Name und das Passwort des Administrator-Benutzers eingegeben werden. Führen Sie folgende Schritte aus um einen Administrator-Benutzer einzurichten. Die Gruppe **FUJITSU SVUSER** und die Benutzer, die dieser Gruppe angehören, werden nicht automatisch erzeugt. Erzeugen Sie eine Gruppe für jeden überwachenden Server und fügen Sie die ServerView Administrator-Benutzer der Gruppe **FUJITSU SVUSER** hinzu.

Ein Administrator-Benutzer in ServerView ist ein Benutzer, der der Gruppe **FUJITSU SVUSER** zugeordnet ist. In Windows Server, werden Administrator-Berechtigungen nicht vergeben, wenn das Passwort der Administrator-Benutzer-Kennung nicht gesetzt ist. Stellen Sie sicher, dass das Passwort gesetzt ist.

Sogar wenn eine "global" Gruppe der Gruppe **FUJITSU SVUSER** hinzugefügt wird, werden die Administrator-Berechtigungen nicht den Benutzern der hinzugefügten Gruppe erteilt. Fügen Sie der **FUJITSU SVUSER** Gruppe nur Benutzer zu. Wird ein Administrator-Benutzer einer anderen Gruppe als **FUJITSU SVUSER** geordnet, wird ein Logon unmittelbar nach Starten des Programms auf Fehler laufen. Klicken Sie in diesem Fall auf **Cancel** um das Logon-Fenster zu schließen.

Legen Sie auf dem Server unter **Properties** auf der Registerkarte **Login** erneut die Anmeldeeinstellungen fest.

1. Öffnen Sie das Control Panel und führen Sie einen Doppelklick auf das Icon **Administrative Tools** aus.
2. Führen Sie einen Doppelklick auf das Icon **Computer Management** aus. Das Fenster **Computer Management** wird geöffnet.
3. Wählen Sie **Local Users and Groups** – **Groups** in der linken Dateibaum-Ansicht.
4. Klicken Sie auf den Menüpunkt **Action** und wählen Sie **New Group...** aus.
5. Tragen Sie **FUJITSU SVUSER** in **Group name** ein und klicken Sie auf **Create**. Eine neue Gruppe wird angelegt. Klicken Sie auf **Close** um das Fenster **New Group** zu schließen.
6. Wählen Sie **Local Users and Groups** – **Users** in der linken Dateibaum-Ansicht.
7. Klicken Sie auf den Menüpunkt **Action** und wählen Sie **New User...** aus.

8. Nehmen Sie die notwendigen Einträge vor und klicken Sie auf **Create**. Ein neuer Benutzer wird angelegt. Klicken Sie auf **Close** um das Fenster **New User** zu schließen.
9. Wählen Sie den hinzugefügten Benutzer aus, klicken Sie auf den Menüpunkt **Action** und wählen Sie **Properties** aus.
10. Klicken Sie auf die Registerkarte **Member of** und klicken Sie auf **Add**. Das Fenster **Select Groups** wird geöffnet.
11. Klicken Sie auf **Properties**.
12. Klicken Sie auf **Search Now**.
13. Wählen Sie die Gruppen **FUJITSU SVUSER** und klicken Sie auf **OK**. Das Fenster **Select Groups** wird erneut geöffnet.
14. Klicken Sie auf **OK**. Die Anzeige kehrt zu dem Fenster **Properties** des Benutzers zurück. Bestätigen Sie, dass **FUJITSU SVUSER** zu **Member of** hinzugefügt wurde und klicken Sie auf **OK**.
15. Klicken Sie auf **OK**. Schließen Sie das Fenster **Computer Management**.

3.6.2 Für Environment mit installiertem Server Core

Im lokalen Konsole-Environment des Server Core, ist das GUI-basierte Management-Tool der Microsoft Management-Konsole (MMC) nicht verfügbar. Führen Sie die folgenden Kommandos aus, um die Gruppe und den Administrator-Benutzer einzutragen.

1. Führen Sie folgendes Kommando aus, um die Gruppe **FUJITSU SVUSER** anzulegen.

   ```
   >net localgroup "FUJITSU SVUSER" /add
   ```

2. Legen Sie einen Administrator-Benutzer an und vergeben Sie ein Passwort.

   ```
   >net user <user name> /add *
   ```

   Nachdem das Kommando ausgeführt wurde, werden Sie aufgefordert ein Passwort einzugeben.

3. Fügen Sie den neu angelegten Benutzer der Gruppe **FUJITSU SVUSER** hinzu.

   ```
   >net localgroup "FUJITSU SVUSER" /add <user name>
   ```

Führen Sie folgende Kommandos aus, um die angelegte Gruppe und den Administrator-Benutzer zu benennen oder zu löschen.

Benennung der Gruppe:

```
>net localgroup "FUJITSU SVUSER"
```

Benennung des Administrator-Benutzers:

```
>net user <user name> /
```

Löschen der Gruppe:

```
>net localgroup "FUJITSU SVUSER" /delete
```

Löschen des Administrator-Benutzers:

```
>net user <user name> /delete
```

3.7 Deinstallation

Dieser Abschnitt erklärt Ihnen, wie Sie den ServerView-Agenten für Windows deinstallieren.

Die Einträge, die im BIOS des Servers gespeichert werden, werden nicht wiederhergestellt, selbst wenn der ServerView-Agent für Windows deinstalliert ist. Stellen Sie den ursprünglichen Zustand der Einstellungen wieder her, und deinstallieren Sie dann den ServerView-Agenten für Windows.

Stellen Sie sicher, dass folgende Schritte befolgt wurden, bevor Sie den ServerView-Agenten für Windows deinstallieren.

1. Setzen Sie die Einstellungen von Software Watchdog, BOOT Watchdog und Power ON/OFF auf Disable.
2. Werden Threshold Monitoring und Report Creation vom Performance Manager verwendet, brechen Sie diese Performances für den Server ab.

Führen sie die folgenden Schritte aus um den ServerView-Agenten für Windows zu deinstallieren.

Sie müssen Windows nicht erneut starten nachdem Sie den ServerView-Agenten für Windows deinstalliert haben.

3.7.1 Windows Server 2008

1. Melden Sie sich als Administrator oder als Benutzer mit Administrator-Rechten an.
2. Beenden Sie alle laufenden Anwendungen.
3. Öffnen Sie das Control Panel und klicken Sie auf **Programs** – **Programs and Features**.
4. Wählen Sie **Fujitsu ServerView Agents** und klicken Sie auf **Uninstall**.

Der ServerView-Agent für Windows wird deinstalliert.

Für Environment mit installiertem Server Core

1. Legen Sie die PRIMERGY Startup Disc ein.
2. Führen Sie die folgende Datei aus.

   <CD/DVD drive>:\PROGRAMS\Japanese2\Svmanage\WinSVAgent\Unagents.bat

3.7.2 Windows Server 2012

1. Melden Sie sich als Administrator oder als Benutzer mit Administrator-Rechten an.
2. Wechseln Sie zur **Start**-Seite von Windows.
3. Starten Sie **Control Panel**.
4. Klicken Sie im Abschnitt **Programs** auf **Uninstall a program**.
5. Wählen Sie **Fujitsu Server View Agents x64 Edition** und klicken Sie auf **Uninstall**.

Der ServerView-Agent für Windows wird deinstalliert.

3.8 Neustart

Der Dienstname der ServerView-Agenten ist **ServerView Server Control**.

Wenn der Dienst neu gestartet wurde, müssen Sie auch den SNMP-Dienst neu starten.

Es wird empfohlen, die Option **Restart Agents** aus dem Menü **Diagnostic Tools** zu verwenden. Über dieses Tool kann sowohl der Dienst **ServerView Server Control** als auch der Dienst **SNMP** neu gestartet werden.